

## UNITED STATES DISTRICT COURT

for the  
Western District of Washington

In the Matter of the Search of  
*(Briefly describe the property to be searched  
 or identify the person by name and address)*  
 Information associated with greenchem201609@hotmail.com  
 that is stored at premises controlled by Microsoft Corporation,  
 more fully described in Attachment A-3.

Case No. MJ19-121

## APPLICATION FOR A SEARCH WARRANT

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property *(identify the person or describe the property to be searched and give its location)*:  
 Information associated with greenchem201609@hotmail.com that is stored at premises controlled by Microsoft Corporation, more fully described in Attachment A-3, incorporated herein by reference.

located in the Western District of Washington, there is now concealed *(identify the person or describe the property to be seized)*:

See Attachments B-3, incorporated herein by reference.

The basis for the search under Fed. R. Crim. P. 41(c) is *(check one or more)*:

- ☒ evidence of a crime;  
☒ contraband, fruits of crime, or other items illegally possessed;  
☒ property designed for use, intended for use, or used in committing a crime;  
☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section	Offense Description
21 U.S.C. §§ 841, 846, 823	Possession with intent to distribute controlled substances; conspiracy to distribute
18 U.S.C. § 1956	controlled substances, distribution of controlled substances by means of the internet; money laundering.

The application is based on these facts:

- ☒ See Affidavit of Special Agent Joseph Cheng, continued on the attached sheet.

☐ Delayed notice of \_\_\_\_\_ days (give exact ending date if more than 30 days: \_\_\_\_\_) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

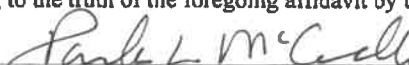
Pursuant to Fed. R. Crim. P. 4.1, this warrant is presented: ☒ by reliable electronic means; or: ☐ telephonically recorded.

  
 Applicant's signature

JOSEPH CHENG, DEA Special Agent  
 Printed name and title

- ☐ The foregoing affidavit was sworn to before me and signed in my presence, or  
☒ The above-named agent provided a sworn statement attesting to the truth of the foregoing affidavit by telephone.

Date: 03/26/2019

  
 Judge's signature

City and state: Bellingham, Washington

PAULA L. MCCANDLIS, United States Magistrate Judge  
 Printed name and title

STATE OF WASHINGTON           )  
  )           SS  
COUNTY OF WHATCOM          )

I, Joseph Cheng, being first duly sworn, hereby depose and state as follows:

1. I am a law enforcement officer of the United States within the meaning of 18 U.S.C. § 2510(7) and empowered by law to conduct investigations of, and to make arrests for, offenses enumerated in 18 U.S.C. § 2516.

2. I am a Special Agent (SA) with the Drug Enforcement Administration (DEA), United States Department of Justice. I have been so employed since August 2006. In connection with my official DEA duties, I investigate criminal violations of the federal narcotics laws, including but not limited to, Title 21, United States Code, Sections 841, 843, 846, and 848. I am currently assigned to the Bellingham Resident Office of the DEA's Seattle Field Division. My current assignment involves investigations of high-level drug trafficking organizations within the Western Washington area and elsewhere.

3. I have completed the DEA Basic Agent Training Course as well as other training courses related to gangs and narcotics trafficking. I have participated in narcotics investigations at both the local and federal level, and I have participated in numerous federal search warrants. As a result, I have become familiar with methods of operation of drug traffickers and organizations. As a Special Agent with the DEA, I have the responsibility of working with other federal and state law enforcement officers in investigations of violations of federal and state controlled substance laws, including the investigation of the distribution of controlled substances including fentanyl and its analogues, cocaine, methylenedioxymethamphetamine (MDMA), methamphetamine, heroin, marijuana, and other dangerous drugs.

1           4. I have interviewed numerous drug dealers, drug users, and knowledgeable  
2 confidential informants about the lifestyles, appearances, and habits of drug dealers and  
3 users. I have become familiar with the manner in which narcotics traffickers smuggle,  
4 package, transport, store, and distribute narcotics, as well as how they collect and launder  
5 drug proceeds. I am also familiar with the manner in which narcotics traffickers use  
6 telephones, cellular telephone technology, internet, pagers, coded communications and  
7 slang-filled conversations, false and fictitious identities, and other means to facilitate their  
8 illegal activities and mislead law enforcement investigations. I have had discussions with  
9 other law enforcement personnel about the packaging and preparation of narcotics, the  
10 methods of illegal narcotics traffickers, and the security measures that narcotics traffickers  
11 often employ. I have examined narcotics customers' supplier lists, pay/owe ledgers  
12 maintained by traffickers, and other documentation related to narcotics trafficking. I have  
13 also examined documentation of various methods by which methamphetamine, cocaine,  
14 marijuana, heroin, and other illicit drugs are smuggled, transported, and distributed. I have  
15 participated in hundreds of hours of surveillance of narcotics traffickers. During  
16 surveillance, I have personally observed narcotics transactions, counter surveillance  
17 techniques, and the ways in which narcotics traffickers conduct clandestine meetings.

18           5. I have also participated in investigations that involved the interception of wire  
19 communications, including four investigations of large-scale drug trafficking organizations  
20 in which I was the case agent and each of which resulted in the conviction of approximately  
21 20 individuals on federal drug-related charges. In addition to these cases, I have participated  
22 in numerous other wiretap investigations in a variety of roles, including by conducting  
23 physical surveillance and monitoring intercepted communications. I have been directly  
24 involved in the review and deciphering of intercepted coded conversations between narcotics  
25 traffickers that were later corroborated by surveillance or by targets' statements. Throughout  
26 my law enforcement career, I have spoken with, worked with, and gained knowledge from  
27 numerous experienced federal, state, and local narcotics officers.

1       6. I have a bachelor's of science in computer science, which I received from San  
2 Jose State University in 2002. During the course of obtaining this degree I completed  
3 courses in network management. Additionally, I have complete college level course work on  
4 computer forensics. During those courses I have learned about network layered architectures  
5 and the principles of network communications using various network protocols.

6       7. I have been assigned as a DEA technical agent since 2010, when I completed  
7 the DEA Basic Technical Course. As part of my duties I have been involved in the searches  
8 of numerous cell phones.

9       8. The facts in this affidavit come from my training, experience, and information  
10 obtained from other agents and witnesses. I have not included every fact known concerning  
11 this investigation. I have set forth the facts that I believe are necessary for a fair  
12 determination of probable cause for the requested search warrants.

## 13                               II. PURPOSE OF AFFIDAVIT

14       9. I make this affidavit in support of an application for search warrants for  
15 information associated with certain accounts (collectively, the "**Target Accounts**") that are  
16 stored at premises controlled by electronic communications service and/or remote computer  
17 service providers, namely, Oath Holdings Inc., formerly Yahoo Holding Inc.; Google LLC,  
18 formerly Google, Inc.; Microsoft Corporation, and eBay (collectively, the "**Service**  
19 **Providers**"), referenced below. The information to be searched is described in the following  
20 paragraphs and in Attachments A, which are incorporated herein. This affidavit is made in  
21 support of an application for search warrants under 18 U.S.C. §§ 2703(a), 2703(b)(1)(A) and  
22 2703(c)(1)(A) to require:

23               a. Oath Holdings Inc., formerly Yahoo Holding Inc. ("Yahoo"), located at  
24 701 First Avenue, Sunnyvale, California, to disclose to the government copies of the  
25 information, including the content of communications, further described in Section I of  
26 Attachment B-1, pertaining to the following Yahoo account, identified in Attachment A-1:  
27 **bradwoolard@ymail.com** ("**Target Account 1**").  
28

b. Google LLC ("Google"), located at 1600 Amphitheater Parkway, Mountain View, California, to disclose to the government copies of the information, including the content of communications, further described in Section I of Attachment B-2, pertaining to the following Google accounts, identified in Attachment A-2: **bradwoolard79@gmail.com** ("Target Account 2") and **broncosmith69@gmail.com** ("Target Account 4").

c. Microsoft Corporation, located at 1 Microsoft Way, Redmond, Washington, to disclose to the government copies of the information, including the content of communications, further described in Section I of Attachment B-3, pertaining to the following Microsoft account, identified in Attachment A-3: **greenchem201609@hotmail.com** ("Target Account 3").

d. eBay, located at 2025 Hamilton Avenue, San Jose, California, to disclose to the government copies of the information, including the content of communications, further described in Section I of Attachment B-4, pertaining to the following eBay accounts, identified in Attachment A-4: **woola-bra** ("Target Account 5") and **wobra.br.kcmtwxi** ("Target Account 6")

10. Upon receipt of the information described in Section I of Attachments B, government-authorized persons will review that information to locate the items described in Section II of Attachments B.

11. Based on my training and experience and the facts set forth in this affidavit, there is probable cause to believe that violations of Title 21, United States Code, Section 841(a) (*distribution of, and possession with intent to distribute, controlled substances*), Title 21, United States Code, Sections 841(a) and 846 (*conspiracy to distribute, and to possess with the intent to distribute, controlled substances*), Title 21, United States Code, Sections 823 and 841(h)(1) (*distribution of controlled substances by means of the*



1 *internet*), Title 21, United States Code, Section 1956 (*money laundering*), and Title 18,  
2 United States Code, Section 922(g) (*felon in possession of a firearm*), have been committed  
3 by Bradley Pete WOOLARD, the user of **Target Account 1**, **Target Account 2**, **Target**  
4 **Account 4**, **Target Account 5**, and **Target Account 6**, as well as others, known and  
5 unknown. There is also probable cause to search the information described in Attachments  
6 A-1, A-2, and A-4, to seize evidence, fruits, and instrumentalities of these crimes further  
7 described in Attachment B-1, B-2, and B-4.

8 12. Based on my training and experience and the facts set forth in this affidavit,  
9 there is probable cause to believe that violations of Title 21, United States Code,  
10 Section 841(a) (*distribution of, and possession with intent to distribute, controlled*  
11 *substances*), Title 21, United States Code, Sections 841(a) and 846 (*conspiracy to distribute,*  
12 *and to possess with the intent to distribute, controlled substances*), Title 21, United States  
13 Code, Sections 823 and 841(h)(1) (*distribution of controlled substances by means of the*  
14 *internet*), and Title 21, United States Code, Section 1956 (*money laundering*), have been  
15 committed by the user of **Target Account 3**, as well as others, known and unknown. There  
16 is also probable cause to search the information described in Attachment A-3 to seize  
17 evidence, fruits, and instrumentalities of these crimes further described in Attachment B-3.

18 13. This Court has jurisdiction to issue the requested warrants because it is “a court  
19 of competent jurisdiction” as defined by 18 U.S.C. §§ 2711, 2703(a), 2703(b)(1)(A) and  
20 2703(c)(1)(A). Specifically, the Court is “in a district court of the United States... that – has  
21 jurisdiction over the offense being investigated.” 18 U.S.C. § 2711(3)(A)(i). Additionally,  
22 with respect to **Target Account 3**, this Court “is in . . . a district in which the provider . . . is  
23 located or in which the wire or electronic communications, records, or other information are  
24 stored.” 18 U.S.C. § 2711(3)(A)(ii).

25 14. Pursuant to 18 U.S.C. § 2703(g), the presence of a law enforcement officer is  
26 not required for the service or execution of this warrant.  
27  
28

### III. SOURCES OF INFORMATION

15. I have obtained the facts set forth in this affidavit from oral and written reports of other law enforcement officers, from records, documents and other evidence obtained during this investigation, and from a confidential source. I have reviewed official reports prepared by other law enforcement officers participating in this investigation and in the other related investigations by agencies referenced in this affidavit.

16. When this affidavit refers to vehicle ownership, either I or other agents involved in the investigation have reviewed the relevant state vehicle records from the Washington State Department of Licensing (“DOL”), or the equivalent agency in other states. Similarly, when I refer to identification documents, either I or other agents involved in the investigation have reviewed the relevant driver license or similar records maintained by DOL or the equivalent agencies in other states. When I refer to the criminal history of a subject, either I or other agents involved in the investigation have reviewed the available criminal history from state or federal agencies. When I refer to telephone subscription records, either I or other agents involved in the investigation have reviewed the subscriber records obtained from the telephone company by administrative subpoena or court order, or I have obtained the information from other law enforcement officers familiar with this investigation. When I refer to telephone toll records, either I or other agents involved in the investigation have received the information from the telephone company pursuant to an administrative subpoena or court authorized pen register/trap and trace device.

### IV. TECHNICAL TERMS AND BACKGROUND

17. Based on my training and experience, and information from other experienced agents, I use the following technical terms to convey the following meanings:

a. “Internet Service Providers” (ISPs) are commercial organizations that are in business to provide individuals and businesses access to the Internet. ISPs provide a range of functions for their customers including access to the Internet, web hosting, email, remote storage, and co-location of computers and other communications equipment.

1           b.       “Internet Protocol address” (IP address), as used herein, is a code made  
2 up of numbers separated by dots that identifies a particular computer on the Internet. Every  
3 computer requires an IP address to connect to the Internet. IP addresses can be dynamic,  
4 meaning that the ISP assigns a different unique number to a computer every time it accesses  
5 the Internet. IP addresses might also be static, if an ISP assigns a user’s computer a  
6 particular IP address which is used each time the computer accesses the Internet.

7           c.       “Domain names” are common, easy to remember names associated with  
8 an IP address. For example, a domain name of “www.usdoj.gov” refers to the IP address of  
9 149.101.1.32. Domain names are typically strings of alphanumeric characters, with each  
10 level delimited by a period.

11           d.       “Website” consists of textual pages of information and associated  
12 graphic images. The textual information is stored in a specific format known as Hyper-Text  
13 Mark-up Language (HTML) and is transmitted from web servers to various web clients via  
14 Hyper-Text Transport Protocol (HTTP).

15           e.       A “Preservation Letter” is a letter governmental entities may issue to  
16 Internet providers pursuant to 18 U.S.C. § 2703(f) to ensure that the Internet Providers  
17 preserve records in its possession. The preservation of such records is necessary given the  
18 dynamic nature of digital records that may be deleted. Based on my training and experience,  
19 and information provided to me from other agents, I know the following:

20           a.       As is the case with most digital technology, communications by way of  
21 computer can be saved or stored on the computer used for these purposes. Storing this  
22 information can be intentional, i.e., by saving an email as a file on the computer or saving the  
23 location of one’s favorite websites in, for example, “bookmarked” files. Digital information  
24 can also be retained unintentionally, e.g., traces of the path of an electronic communication  
25 may be automatically stored in many places (e.g., temporary files or ISP client software,  
26 among others). In addition to electronic communications, a computer user’s Internet  
27 activities generally leave traces or “footprints” in the web cache and history files of the  
28 browser used. A forensic examiner often can recover evidence suggesting whether a



1 computer contains peer to peer software, when the computer was sharing files, and some of  
2 the files which were uploaded or downloaded. Such information is often maintained  
3 indefinitely until overwritten by other data.

4           b.       **Email and Data Storage:** In general, an email that is sent to a  
5 subscriber of the service provider is stored in the subscriber's "in-box" on the service  
6 provider's servers until the subscriber deletes the email. If the subscriber does not delete the  
7 message, the message can remain on service provider's servers indefinitely. The user can  
8 move and store messages in personal folders such as a "sent folder." In recent years, the  
9 service provider and other ISPs have provided their users with larger storage capabilities  
10 associated with their users' email account. ISPs, including the service provider, provide  
11 users with as much as multiple gigabytes of online storage space. Based on my experience  
12 and conversations with other law enforcement officers with experience in executing and  
13 reviewing search warrants of email accounts, I have learned that search warrants for email  
14 accounts and computer systems have revealed stored emails sent and/or received many years  
15 prior to the date of the search. The service provider also provides subscribers with various  
16 other associated products and services in connection with their accounts, including chat  
17 programs, photo and video sharing platforms and other services or social media programs.

18           c.       **Data Retention:** When the subscriber sends an email, it is initiated at  
19 the user's computer or other internet access device, transferred via the Internet to the service  
20 provider's servers, and then transmitted to its end destination. The service provider often  
21 saves a copy of the email sent. Unless the sender of the email specifically deletes the email  
22 from the service provider's servers, the email can remain on the system indefinitely.

23           d.       **Email Messages:** A sent or received email typically includes the  
24 content of the message, source and destination addresses, the date and time at which the  
25 email was sent, and the size and length of the email. If an email user writes a draft message  
26 but does not send it, that message may also be saved by the service provider but may not  
27 include all of these categories of data.

1           e.     **Online Data Storage:** A subscriber of the service provider can also  
2 store files, including emails, address books, contact or buddy lists, calendar data, pictures,  
3 and other files on servers maintained and/or owned by the service provider. Subscribers to  
4 the service provider might not store on their home computers copies of the emails stored in  
5 the Target Account. This is particularly true when they access the Target Account through  
6 the web, or if they do not wish to maintain particular emails or files in their residence. In  
7 essence, a subscriber's email box has become a common online data storage location for  
8 many users. This is particularly true when they access the Target Account through the web,  
9 or if they do not wish to maintain particular emails or files in their residence.

10           f.     **Identifying Information:** In general, email providers such as the  
11 service provider ask each of their subscribers to provide certain personal identifying  
12 information when registering for an email account. This information could include the  
13 subscriber's full name, physical address, telephone numbers and other identifiers, such as  
14 alternative email addresses, and, for paying subscribers, means and source of payment  
15 (including any credit or bank account number).

16           g.     **Transactional Information:** Service providers typically retain certain  
17 transaction information about the creation and use of each account on their systems. This  
18 information can include the date on which the account was created, the length of service,  
19 records of log-in (i.e., session) times and durations, the types of service utilized, the status of  
20 the account (including whether the account is inactive or closed), the methods used to  
21 connect to the account (such as logging into the account via service provider's website), and  
22 other log files that reflect usage of the account. In addition, email providers often have  
23 records of the IP address used to register the account and the IP addresses associated with  
24 particular logins to the account. Because every device that connects to the Internet must use  
25 an IP address, IP address information can help to identify which computers or other devices  
26 were used to access the email account.

27           h.     **Technical Support:** In some cases, account users will communicate  
28 directly with a service provider about issues relating to the account, such as technical

1 problems, billing inquiries, or complaints from other users. Service providers typically  
 2 retain records about such communications, including records of contacts between the user  
 3 and the providers support services, as well as records of any actions taken by the provider or  
 4 user as a result of the communications.

5 i. **Attribution Evidence:** In my training and experience, evidence of who  
 6 was using an account may be found in address books, calendars, contact or buddy lists,  
 7 emails in the account, and attachments to emails, including pictures and files.

## 8 V. SUMMARY OF PROBABLE CAUSE

9 18. An ongoing investigation is being conducted by the Drug Enforcement  
 10 Administration (DEA) into the importation of pure powdered fentanyl and its analogues by  
 11 WOOLARD, and others, both known and unknown. Investigators believe that WOOLARD  
 12 (and, possibly, others) ordered the fentanyl and its analogues over the internet from China.  
 13 Once WOOLARD and/or his coconspirators received the powdered fentanyl through the  
 14 mail, WOOLARD caused the fentanyl to be pressed into fentanyl-laced counterfeit  
 15 oxycodone pills. Once pressed into pills, WOOLARD and others distributed these  
 16 dangerous pills into the community.

17 19. In July and August 2018, investigators executed multiple federal search  
 18 warrants of WOOLARD's residence, located at 9717 99<sup>th</sup> Avenue Northeast, Arlington,  
 19 Washington (hereinafter, the "WOOLARD Residence"). Pursuant to those search warrants,  
 20 investigators seized approximately 10,000 light blue pills marked "M30" which tested  
 21 positive for furanyl fentanyl, a fentanyl analogue. Investigators seized numerous items  
 22 during the searches of the WOOLARD Residence and outbuildings, including 33 firearms  
 23 (the majority of which were concealed in a hidden room in a shop on the property),  
 24 thousands of rounds of ammunition, approximately \$1.1 million in suspected drug proceeds  
 25 concealed in various locations throughout the WOOLARD Residence and in the shop areas  
 26 on the property, and cell phones, including an Apple iPhone. Investigators seized multiple  
 27 documents from the WOOLARD Residence referencing (360) 395-5222 and  
 28 bradwoolard79@gmail.com (**Target Account 2**) as being used by WOOLARD.

1           20. Investigators searched the iPhone seized from the WOOLARD Residence  
 2 pursuant to search warrants. Investigators learned this iPhone was assigned (360) 395-5222  
 3 and Apple ID bradwoolard@ymail.com (**Target Account 1**). Two email accounts were  
 4 synced with this iPhone, bradwoolard@ymail.com (**Target Account 1**) and  
 5 bradwoolard79@gmail.com (**Target Account 2**). Review of emails on this phone revealed  
 6 email exchanges between WOOLARD, using **Target Account 2**, and individuals who  
 7 appeared to be based in China. In these emails, WOOLARD and the China-based  
 8 individuals openly discussed WOOLARD attempting to obtain various chemical substances,  
 9 including fentanyl and furanyl fentanyl, from China.

10           21. Investigators have reviewed business records from eBay that indicate that  
 11 WOOLARD had two eBay accounts. WOOLARD used bradwoolard79@gmail.com  
 12 (**Target Account 2**) as part of his registration for his eBay account associated with the user  
 13 ID “wobra.br.kcmtwxi” (**Target Account 6**). WOOLARD used bradwoolard@ymail.com  
 14 (**Target Account 1**) as part of his registration for his eBay account associated with the user  
 15 ID “woola-bra” (**Target Account 5**). According to eBay, WOOLARD used the former eBay  
 16 account to purchase molds for a pill press, and the latter to purchase molds for multiple types  
 17 of pills and a pill press machine.

18           22. According to records obtained from PayPal, WOOLARD has two separate  
 19 PayPal accounts in the name Bradley WOOLARD with the email address of  
 20 bradwoolard79@gmail.com (**Target Account 2**). According to PayPal records, on  
 21 February 8, 2016, WOOLARD sent a payment of \$1,710.80 to pay for a pill press machine  
 22 that WOOLARD had shipped to “Keith Strand, 1443 Lake Dr., Camano Island, WA 98282.”

23           23. Investigators obtained a federal search warrant for WOOLARD’s iCloud  
 24 account, for which WOOLARD’s Apple ID is bradwoolard@ymail.com (**Target**  
 25 **Account 1**). During a review of WOOLARD’s iCloud account, investigators found one  
 26 photo of a partially compressed email exchange in which an individual using the moniker  
 27 “Mary” and email address greenchem201609@hotmail.com (**Target Account 3**), directed  
 28 the user of email address broncosmith69@gmail.com (**Target Account 4**) to transfer \$2,700

1 to “Fengjun Huang” in China. During this email exchange, the user of email address  
 2 broncosmith69@gmail.com (**Target Account 4**) wrote, “Pkg 4 is still in China after a  
 3 month.”

4 24. Investigators found communications between “Mary,” using  
 5 greenchem201609@hotmail.com (**Target Account 3**), and “Bronco Smith,” during a search  
 6 of WOOLARD’s seized iPad mini pursuant to a federal search warrant. Based review of the  
 7 photographs found in WOOLARD’s iPad mini, investigators believe that that WOOLARD  
 8 was the user of broncosmith69@gmail.com (**Target Account 4**).

9 25. In light of the investigation to date, to include the seizures from the  
 10 WOOLARD Residence, WOOLARD’s known use of email to further his criminal offenses,  
 11 and the records discussed herein, I believe evidence concerning WOOLARD’s above-  
 12 referenced criminal offenses will be found in all of the **Target Accounts**. Additionally, I  
 13 **Target Account 3** is being used by a China-based source of supply for fentanyl and its  
 14 analogues to communicate regarding payment for, and distribution of, these controlled  
 15 substances with WOOLARD and others, as yet unknown.

## 16 VI. PROBABLE CAUSE

### 17 A. The Investigation

18 26. As discussed herein, DEA is investigating fentanyl trafficking and related  
 19 offenses in the Western District of Washington and elsewhere, by Bradley WOOLARD and  
 20 his criminal associates. The investigation is ongoing. Based on my training and experience,  
 21 and information relayed to me by other law enforcement personnel, I know that fentanyl is a  
 22 Schedule II narcotic and a highly a dangerous drug. Fentanyl is a synthetic opioid that is 50  
 23 times more toxic than heroin. In its purest form fentanyl is a white powder or in grains  
 24 similar in size to table salt. For most people, two to three milligrams of fentanyl is capable  
 25 of inducing respiratory depression, arrest and possibly death. Two to three milligrams of  
 26 fentanyl is comparable in size to five to seven individual grains of table salt. Additionally,  
 27 counterfeit Percocet pills have been associated with multiple overdose deaths in Skagit and  
 28



1 Snohomish Counties in 2018 and fentanyl has been linked to multiple overdoses in  
2 Snohomish County, Washington.

3 27. Based on my training and experience, I know that 100 grams of fentanyl, when  
4 pressed with binding material such as cellulose or gypsum, can be used to make  
5 approximately 100,000 counterfeit/fake Oxycodone pills, with a value ranging between  
6 \$1,200,000 and \$3,000,000.

7 ***July 2018 - Traffic Stop of Griffin THOMPSON***

8 28. As part of law enforcement's ongoing investigation, investigators conducted  
9 surveillance at Griffin THOMPSON's residence, located at 1404 East 36<sup>th</sup> Lane, Bellingham,  
10 Washington (hereinafter, the "THOMPSON Residence")<sup>1</sup> on July 27, 2018. At  
11 approximately 8:45 p.m., investigators observed the gray Toyota 4 Runner depart  
12 THOMPSON's Residence with two occupants. Investigators, with the assistance of a law  
13 enforcement helicopter, followed the gray Toyota 4 Runner as it drove south to Arlington,  
14 Washington. At approximately 9:38 p.m., investigators observed the gray Toyota 4 Runner  
15 park near the Safeway, located at 20500 Olympic Place, Arlington, Washington.  
16 Investigators then observed the passenger get out of the gray Toyota 4 Runner, access the  
17 back of the vehicle and walk away from the vehicle. The driver of the vehicle was not  
18 observed getting out of the vehicle at that location. Investigators then observed the gray  
19 Toyota 4 Runner depart Safeway and drive south.

20 29. Investigators followed the gray Toyota 4 Runner until it parked in front of a  
21 residence located at 9717 99<sup>th</sup> Avenue Northeast, Arlington, Washington (the WOOLARD  
22 Residence), at approximately 9:45 p.m. Investigators then observed the driver of the vehicle  
23 walk into the front door of the WOOLARD Residence. Approximately six minutes later at  
24 9:51 p.m., investigators observed the gray Toyota 4 Runner pull out of the WOOLARD  
25 Residence.

26  
27  
28 <sup>1</sup> According to the Washington Department of Licensing, Griffin THOMPSON's address on his Washington driver's  
license is 1404 East 36<sup>th</sup> Lane Bellingham, Washington.

1           30. Investigators continued to follow the gray Toyota 4 Runner as it arrived at the  
2 same Safeway at approximately 10:03 p.m. Prior to the arrival of the gray Toyota 4 Runner,  
3 investigators observed the female, subsequently identified as Mikala MURPHY, sitting in  
4 front of the Safeway. Investigators did not observe anything in MURPHY's hands at that  
5 time. Investigators observed MURPHY get into the gray Toyota 4 Runner and depart the  
6 Safeway. Investigators followed the gray Toyota 4 Runner until a traffic stop was conducted  
7 on the vehicle for suspicion of involvement in drug trafficking activity. At that time, the  
8 driver of the vehicle was positively identified as Griffin THOMPSON, via his Washington  
9 driver's license and the passenger was identified as Mikala MURPHY, via her U.S. passport.

10           31. Soon after the traffic stop, a narcotics detecting K-9 was deployed to sniff the  
11 exterior of the vehicle and gave a positive alert to the odor of narcotics emanating from the  
12 vehicle. Investigators then subsequently searched the vehicle pursuant to the vehicle  
13 exception. During that search, investigators located and seized from underneath the front  
14 passenger seat (in an area that could only be accessed from the rear seats) a white box which  
15 contained 3 ziploc baggies of light blue colored pills marked "M30." An open-source  
16 internet search indicated that pills marked "M30" are 30 milligram Oxycodone. Oxycodone  
17 is a Schedule II narcotic. These pills were sent to the DEA laboratory for testing and the  
18 laboratory counted 3,137 pills and indicated that they tested positive for furanyl fentanyl,  
19 which is a fentanyl analogue. During a pat-down of THOMPSON's person, approximately  
20 \$8,122 of U.S. currency was recovered.

21           32. Investigators advised THOMPSON of his rights and he stated that he wished to  
22 speak to an attorney. No further questions were asked of THOMPSON. Investigators  
23 advised MURPHY of her rights, which she waived. MURPHY stated she had been dropped  
24 off at a Safeway by her boyfriend, THOMPSON. THOMPSON was driving MURPHY  
25 home to her residence in Lake Stevens, Washington. MURPHY stated she had to use the  
26 restroom and THOMPSON told her he needed to go run an errand and would be back shortly  
27 to pick her up. MURPHY stated THOMPSON dropped her off and left the area. MURPHY  
28 said that THOMPSON took longer than she anticipated, and she began texting him telling

1 him to hurry up and return to pick her up. MURPHY stated when he returned, he began  
2 driving towards her residence to take her home.

3 33. THOMPSON and MURPHY were booked into Snohomish county jail on drug  
4 trafficking charges and were later released.

5 34. During the pat-down of THOMPSON's person, an Apple iPhone was located.  
6 An LG cell phone, along with indicia documents for THOMPSON were found in a black  
7 backpack in the back of the gray Toyota 4 Runner. An additional Apple iPhone was also  
8 found in the 4 Runner. All three cell phone were seized in anticipation of obtaining a search  
9 warrant.

10 35. On July 31, 2018, U.S. Magistrate Judge Donohue issued a federal search  
11 warrant authorizing the search of the three cell phones seized from THOMPSON and  
12 MURPHY. Pursuant to that search warrant, investigators identified the phone numbers of  
13 the devices as follows: the iPhone found on THOMPSON's person was assigned 425-923-  
14 6287; the other iPhone was assigned 425-870-7343; and the LG cell phone was assigned  
15 206-200-9833. Investigators attempted to search 425-923-9287 but the phone was passcode  
16 protected and locked.

17 36. Toll records obtained from Verizon show that this phone (425-923-6287) is  
18 subscribed to "Virginia Baldwin" at 1404 East 36<sup>th</sup> Lane, Bellingham, Washington  
19 (THOMPSON's Residence). Additionally, as discussed below, 425-923-6287 was stored in  
20 Adrian BERGSTROM's phone under the name "Griffin," which THOMPSON's first name.

21 37. Investigators were able to search the LG phone (206-200-9833) pursuant to  
22 the warrant. During the search, investigators saw a text sent on May 4, 2018, stating "Hey  
23 whats up this is G this is my work phone." Based on where the LG phone was found, and  
24 this text message, investigators believe to be Griffin THOMPSON to be the user of 206-200-  
25 9833.

***July and August 2018 – Investigators Execute Multiple Search Warrants of the WOOLARD Residence***

38. On July 28, 2018, the Honorable Mary Alice Theiler signed a search warrant authorizing the search of 9717 99<sup>th</sup> Avenue Northeast, Arlington, Washington (the WOOLARD Residence), *i.e.*, the residence of WOOLARD, Shawna Marie Bruns (WOOLARD's wife), and their minor children. During the execution of the search warrant that day, investigators found approximately 10,000 of the counterfeit Percocet pills located in the office of the main residence. In this office, there were numerous documents with the name Bradley WOOLARD. Additionally seized from the office was a small container of blue dye, which investigators suspect could have been used by WOOLARD in the process of pressing white fentanyl powder and binding materials into counterfeit M30 pills. The pills located in the office were consistent with the appearance of the pills seized from THOMPSON on July 27, 2018. These pills were submitted to the DEA laboratory for testing and the laboratory counted 12,389 pills and indicated that they tested positive for furanyl fentanyl.

39. Investigators also found approximately \$400,000 in cash located in two safes, one in the office and one in the master bedroom closet. Items of dominion and control with WOOLARD's name were found in the office and master bedroom.

40. WOOLARD also had four high valued vehicles at the address, including a 2014 Nissan GTR, registered to Fun Times Trust at the WOOLARD Residence, valued at approximately \$100,000, a 2017 Harley Davidson motorbike, valued at approximately \$25,000, a 1965 Chevrolet Nova valued at approximately \$35,000, and a 2017 GMC Denali, valued at approximately \$65,000.<sup>2</sup>

---

<sup>2</sup> On July 30, 2018, U.S. Magistrate Judge Mary Alice Theiler signed a warrant authorizing the searches of two additional residences which were owned by WOOLARD. These addresses were 9019 99<sup>th</sup> Avenue Northeast, Arlington, Washington, and 1929 201<sup>st</sup> Place South West, Lynnwood, Washington. On July 31, 2018, investigators executed both search warrants. No evidence of drug trafficking was found at either location.

1           41. During the search on July 28, 2018, investigators found a receipt for a Western  
2 Union Receipt in the master bedroom closet. According to the receipt, the receipt was for a  
3 money transfer, with Western Union tracking number (MTCN) 3920127463, made by sender  
4 Keith STRAND, 1443 Lake Drive, Camano Island, WA 98282, on July 17, 2017, from the  
5 Rite Aid located at 26817 88<sup>th</sup> Avenue NW, Stanwood, WA 98292-9811, to Fengjun Huang  
6 in China. The amount of funds transferred was \$900.

7           42. Additionally, during the July 28 search of the WOOLARD Residence,  
8 investigators seized two shipping labels from the trash in the office. One shipping label had  
9 the sender and recipient removed but described the contents as "Lab supplies" with a weight  
10 of 0.1 kilograms, a value of \$5.00 and goods' origin of "CN". A second shipping label was  
11 largely intact and also listed the contents as "Lab supplies" with the same weight, value and  
12 goods' origin. This shipping label showed "Danette Skelton" and "32326 Mountain Loop  
13 Hyway, Granite Falls WA USA 98252" as the "ship to" information and the "from"  
14 information listed "Wuzong Hui" and "China 61 Jianning Road No. 3 Building 1502 Room  
15 GulouQu, Nanjing Jiangsu 210000." Additionally the shipping labels listed tracking number  
16 LS508043116CN. According to the USPS website, this package was delivered to the  
17 Granite Falls address on January 29, 2018.

18           43. During the search on July 28, 2018, investigators observed a computer in the  
19 WOOLARD Residence, which was not within the scope of the search warrant and was not  
20 seized. As discussed throughout this affidavit, investigators believe that fentanyl and its  
21 analogues such as furanyl fentanyl are being sourced from China. Based on my training and  
22 experience, I know that computers are frequently used to buy items online and to  
23 communicate with others located in foreign countries when a language barrier might be  
24 present.

25           44. On August 16, 2018, the computer and other digital devices present in the  
26 WOOLARD Residence, including an Apple iPhone, were seized pursuant to a federal search  
27 warrant that had been issued by U.S. Magistrate Judge Paula L. McCandlis on August 15,  
28 2018. Searches of WOOLARD's iPhone are discussed below. Investigators sent two



1 computers and two iPad minis seized from the WOOLARD Residence to law enforcement  
 2 (DEA and FBI) computer forensics labs to be searched. Investigators have received the  
 3 analysis of one of the iPad minis and are reviewing the records; investigators are awaiting  
 4 the results of the other devices. The search of this iPad is discussed in further in this  
 5 affidavit.

6 45. On August 18, 2018, a confidential source (hereinafter CS2) contacted  
 7 SRDGTF detectives and stated s/he had information regarding the WOOLARD Residence.  
 8 CS2 has no criminal history and works closely with law enforcement in the local Snohomish  
 9 County area. CS2 has had traffic violations, but nothing within the last five years. CS2 is  
 10 seeking employment with law enforcement.

11 46. CS2 stated s/he had known Matthew EDWARDS,<sup>3</sup> a friend of Bradley  
 12 WOOLARDS, since 2016. EDWARDS had reached out to CS2 via text on August 18, 2018,  
 13 and stated the two of them needed to talk. The phone number that CS2 communicated with  
 14 was the number that EDWARDS had given investigators on July 31, 2018: (253) 306-2473.

15 47. Investigators met with CS2 and reviewed the text communications between  
 16 CS2 and the number (253) 306-2473. Investigators preserved the text communications by  
 17 taking photographs of them. Below is a portion of the text string between CS2 and  
 18 EDWARDS:

19 EDWARDS: 'We need to talk'

20 CS2: 'Okay about what?'

21 EDWARDS: 'U an me are about to have a lot of \$'

22 CS2: Oh boy. I like this.. who's driving?'

23 EDWARDS: 'It's gonna have to be at night at the location I been going to.'

24 EDWARDS: 'And it's gonna take some work to get it out?'

25  
 26 <sup>3</sup> On July 31, 2018, during the execution of the federal search warrant at 9019 99<sup>th</sup> Avenue North East, Arlington, WA,  
 27 an address associated with WOOLARD, Matthew EDWARDS approached SA Burford and stated he was good friends  
 28 with 'Shawna', WOOLARD's wife. EDWARDS stated he had no knowledge of WOOLARD's activity, but did provide  
 a phone number for WOOLARD, *i.e.*, (360) 395-5222. EDWARDS provided his phone number as (253) 306-2473.

1 CS2: 'What are we doing'

2 CS2: 'That safe?'

3 EDWARDS: 'No not the safe in a wall'

4 EDWARDS: '5 to 6 million no lie I'm the only one that knows we're gonna take a  
5 small portion for ourselves and get it for Someone'

6 48. CS2 stated EDWARDS then called him/her and stated EDWARDS planned to  
7 return from Cle Elum, Washington on August 19, 2018, and the two of them would go to the  
8 WOOLARD Residence and remove the money during the night. CS2 stated EDWARDS  
9 told him/her that "Shawna," known to investigators as Shawna BRUNS, had reached out to  
10 EDWARDS and stated the police did not find the 5 million dollars, which was located in a  
11 wall behind a towel rack. EDWARDS told CS2 that "Shawna" was leaving WOOLARD  
12 and needed someone to go back to the residence and remove the money and bring it to her.  
13 EDWARDS further related to CS2 that "Shawna" would split some of the money with  
14 EDWARDS. EDWARDS told CS2 if the amount of money was more than 5 million dollars,  
15 that they would just take the extra before turning it over to "Shawna." CS2 stated  
16 EDWARDS did not share the specific location of where the money was hidden, just that it  
17 was in the wall behind a towel rack.

18 49. In the late evening of August 18, 2018, members of SRDGTF executed a  
19 federal search warrant at the WOOLARD Residence, which had been authorized by the  
20 Honorable David W. Christel earlier that day. During this search of the WOOLARD  
21 Residence, investigators located approximately \$6,000 U.S. Currency and a cell phone,  
22 which was in a container disguised as a book, that were concealed under kickboard in the  
23 master bathroom. To access this area, which was not readily accessible, investigators had to  
24 cut into the base of the cabinets in the master bathroom. This cell phone was searched  
25 pursuant to the warrant, and agents located texts between the user of the cell phone and an  
26 individual using the number (425) 263-6876. In a text, the user of (425) 263-6876 gave her  
27 name as Danette Skelton and her address 32326 Mt Loop Hwy Granite Falls, WA – the same  
28 addressee and address on the packaging found in the trash at the WOOLARD Residence on

1 July 28, 2018. Other texts between these two phones appear to discuss a parcel, which  
2 investigators suspect contained fentanyl.

3 50. On September 6, 2018, agents interviewed SKELTON. She gave the agents  
4 her phone number, which was (425) 263-6876. The following day, agents again contacted  
5 SKELTON and seized that phone.

6 51. During the search of the WOOLARD Residence on August 18, 2018, three  
7 firearms were also located in the attic. These firearms were in the ceiling insulation.  
8 Because of the late hour, the WOOLARD Residence was secured overnight by the SRDGT  
9 until August 19, 2018. During daylight hours on August 19, 2018, the search continued and  
10 agents located approximately \$270,000.00 U.S. Currency, which was located in airtight,  
11 plastic receptacles. One receptacle contained approximately \$100,000.00 U.S. Currency,  
12 was located in the insulation, behind the water heater in the southeast shop. The second,  
13 similar receptacle, was located in the back of a tool chest in the same shop. The third  
14 receptacle, was located in the bottom drawer of a dehydrator. The dehydrator was located in  
15 the northeast shop.

16 52. Additionally, multiple weapons were located in a concealed room in the loft of  
17 the southeast shop, hidden behind a metal wall locker. This concealed room shares a wall  
18 with the second floor of the adjoining apartment. The weapons varied from assault rifles to  
19 pistols with homemade silencers. The Bureau of Alcohol, Tobacco, Firearms, and  
20 Explosives assisted with the seizure of these weapons and thousands of rounds of live  
21 ammunition.

22 53. During the course of the search, CS2 attempted to elicit information from  
23 BRUNS as to the locations of where the money was on the property. BRUNS told CS2 there  
24 was some money in the house, but there were other various locations throughout the property  
25 that "Bradley", known to investigators as WOOLARD, hid money. BRUNS told CS2 she  
26 still wanted EDWARDS and other individuals to go to the residence to retrieve the money  
27 for her after law enforcement left the location.

1        54. At approximately 7:16 p.m., investigators placed surveillance team members in  
2 the wood line of the property to maintain positive control of the WOOLARD Residence with  
3 law enforcement presence.

4        55. During the evening of August 19, 2018, CS2 provided information that three  
5 individuals would be responding to the WOOLARD Residence with intentions of locating  
6 hidden currency throughout the property. At approximately 9:22 p.m., a dark colored SUV  
7 arrived with three male occupants, later identified as EDWARDS, and two other individuals.  
8 Onsite surveillance team members observed the targets enter the main residence briefly, and  
9 then move to the rear of the property. The targets entered both the northeast and southeast  
10 shops and returned to the SUV a short time later. They appeared to load items into the  
11 vehicle. The three targets reentered the SUV at which point the vehicle proceeded to the  
12 exit. Surveillance members intercepted the SUV prior to it exiting onto 99<sup>th</sup> Avenue North  
13 East. All occupants were detained without incident.

14        56. The SUV was subsequently searched using the automobile exception. During  
15 the search of the vehicle, approximately \$60,000 U.S. Currency was located under the  
16 passenger seat along with two, plastic bottles containing gold coins. These plastic bottles  
17 had a durable string approximately 12 inches in length wrapped around the top of the bottle.  
18 Located under the driver seat was approximately \$50,000 U.S. Currency.

19        57. EDWARDS was advised of his legal rights, which he waived. EDWARDS  
20 stated that "Shawna" had requested him, and the two other individuals respond to the  
21 WOOLARD Residence and retrieve items for her children as well as hidden U.S. Currency.  
22 EDWARDS said "Shawna" provided specific locations for them to check. EDWARDS said  
23 upon arrival, one of the other individuals entered the main residence and returned a short  
24 time later, and the three individuals proceeded to the two shops where the U.S. Currency was  
25 located. EDWARDS stated the three of them entered into the apartment in the southeast  
26 shop, where "Shawna" gave them instructions to look behind the toilet paper roll for the  
27 string which would allow access to the gold and U.S. Currency which was concealed behind  
28 drywall. EDWARDS also relayed that "Shawna" told them to look in the insulation in the

1 northeast shop, as U.S. Currency was located in various locations. EDWARDS told  
2 investigators he believed there was additional money hidden in the walls of the apartment in  
3 the southeast shop.

4 58. Based on new information, on August 20, 2018 and August 22, 2018, the  
5 Honorable Judge Paula L. McCandlis signed search warrants authorizing the search of the  
6 WOOLARD Residence. During the resulting searches, approximately \$100,000 in U.S.  
7 Currency was located in the northwest shop, on top of the support beam, and in the rafters in  
8 insulation, and approximately \$200,000 in U.S Currency was located, hidden behind the  
9 dishwasher in the WOOLARD Residence.

10 ***Two Packages of Fentanyl Shipped from China Intercepted by Law Enforcement***

11 59. As discussed above, the shipping labels found in the WOOLARD Residence  
12 listed the "from" information as "Wuzong Hui" and "China 61 Jianning Road No. 3 Building  
13 1502 Room GulouQu, Nanjing Jiangsu 210000." Investigators identified two additional  
14 parcels that were en route to Western Washington from the same shipper as listed on  
15 packaging materials found in the WOOLARD Residence. Both parcels were intercepted.  
16 On August 2, 2018, investigators obtained federal search warrants for the two additional  
17 parcels, one of which was addressed to Sadie BATES at 12118 Hwy 99 #J 402, Everett,  
18 Washington, and one of which was addressed to Adrian BERGSTROM at 200 East Maple St  
19 Apt 507, Bellingham USA US 98225.

20 60. The parcels were searched pursuant to the warrant. Inspector Myhrer used the  
21 TruNarc Handheld Narcotics Analyzer on the contents of the packages. Both packages  
22 yielded a presumptive positive result for fentanyl. A TruNarc Handheld Narcotics Analyzer  
23 uses Raman spectroscopy to identify narcotics, stimulants, depressants, hallucinogens and  
24 analgesics. The contents of both packages were submitted to the DEA laboratory for testing.  
25 According to the DEA lab, the contents of both parcels tested positive for furanyl fentanyl  
26 and weighed approximately 99.4 grams and 99.6 grams.



1       61. On August 3, 2018, U.S. Magistrate Judge Christel issued anticipatory search  
2 warrants, including a warrant for 200 East Maple St Apt 507, Bellingham, Washington,  
3 contingent upon the delivery of the parcel to that location.

4       62. On August 6, 2018, a controlled delivery of the parcel addressed to Adrian  
5 BERGSTROM was conducted. During that controlled delivery, investigators detained  
6 BERGSTROM as he was walking away from his residence and seized his cell phone.  
7 BERGSTROM consented to a search of his cell phone.

8       63. Investigators identified two phone numbers stored in BERGSTROM's cell  
9 phone which are believed to be used by Griffin THOMPSON: stored under the name "Griff"  
10 was the number (425) 293-6782, and stored under the name "Griffin" was (425) 923-6287.

11       64. Additionally, toll records obtained from Verizon for (425) 293-6782 show that  
12 this phone is subscribed to Griffin THOMPSON at 1404 East 36<sup>th</sup> Lane, Bellingham, WA  
13 (THOMPSON Residence) and on August 1, 2018 THOMPSON used (425) 293-6782 to send  
14 a picture message (MMS) to himself at griffin.thompson@gmail.com. In this way,  
15 investigators identified this email as used by THOMPSON.

16       65. On August 14, 2018, United States Magistrate Judge Paula McCandlis issued  
17 search warrants for four locations, including 1404 East 36<sup>th</sup> Lane, Bellingham, Washington  
18 (the THOMPSON Residence). Agents seized multiple digital devices from the residence, as  
19 well as digital scales which contained suspected drug residue and resealable plastic baggies  
20 containing suspected drug residue.

21 ***Searches of WOOLARD's iPhone***

22       66. On August 28 and 29, 2018, pursuant to a federal search warrant, agents  
23 reviewed the contents of the iPhone seized from the WOOLARD Residence on August 16,  
24 2018. As noted above, the number for this iPhone is (360) 395-5222. I also observed there  
25 was an email account, bradwoolard79@gmail.com (**Target Account 2**) saved to the iPhone.

26       67. Review of text messages stored on WOOLARD's iPhone revealed numerous  
27 text messages pertaining to distribution of "blues" (slang for M30 Oxycodone pills), the  
28 manufacture and distribution of marijuana, and construction/remodeling. For example, on

1 June 8, 2012, an individual whose phone number was stored under the name "Mo" sent  
2 WOOLARD, "Couple blues?" On June 12, 2012, "Trevor A" sent "are the blue's around big  
3 daddy?", and WOOLARD replied, "I not sure I'll see." Based on my training and  
4 experience and the light blue color of the counterfeit "M30" pills seized from WOOLARD's  
5 residence I believe that "Mo" and "Trevor A" were asking WOOLARD if he had "M30s"  
6 available and that WOOLARD has been involved in distributing "M30" pills since at least  
7 June of 2012.

8 68. Additional text messages show that "Devin" or one of "Devin's" associates  
9 was one of WOOLARD's sources of supply at that time. Specifically, on July 1, 2012,  
10 WOOLARD asked "Devin," "Do u bro have any blues." "Devin" replied, "Still trying to get  
11 ahold of my brother was supposed to meet up with him last night" and "how mutch do u  
12 want if I get ahold of him" and WOOLARD replied, "like 5" and "If they r the m brand  
13 more." On the same day, WOOLARD asked another person, with no contact name saved  
14 using 425-319-5980, "hey b do you know anyone wit a 50 pack or a pack of blues there  
15 trying to get rid of, my friend js looking." 425-319-5980 replied, "Not for cheep."  
16 WOOLARD then asked, "what is the price?" and 425-319-5980 replied, "I'll ask." Based on  
17 my training and experience, I believe that WOOLARD is trying to obtain "blues" or "M30"  
18 pills for his customers. A further review of this iPhone showed that WOOLARD and various  
19 other individuals continue to exchange messages about "blues" through the duration of the  
20 time period (June 2012 through August 2014) for which text messages are stored on this  
21 iPhone.

22 69. During a review of the email stored on WOOLARD's iPhone, pursuant to the  
23 warrant, I observed emails between WOOLARD and an individual in which WOOLARD  
24 and that individual appeared to be discussing the purchase of fentanyl. The other individuals  
25 indicated that they could provide the fentanyl. After I observed the email contents, I  
26 determined that extensive electronic evidence may be stored on this iPhone and other digital  
27 devices regarding communications with suppliers of fentanyl in China and records of internet  
28

1 purchases of fentanyl, which may involve violations of 21 U.S.C. §§ 823, 841(g), 841(b)(1)  
2 and 846 (distribution of controlled substances by means of the internet).

3 70. In an abundance of caution, agents ceased their review of the email content  
4 stored on WOOLARD's iPhone, and applied for a search warrant to gather evidence with  
5 respect to the crime of distribution of controlled substances by means of the internet and  
6 related offenses (violations of 21 U.S.C. § 841(a)(1) and 846, 18 U.S.C. § 1956, and 18  
7 U.S.C. § 922(g)), for WOOLARD's iPhone as well as for other digital devices previously  
8 seized. U.S. Magistrate Judge McCandlis issued the requested search warrant on October 5,  
9 2018.

10 71. WOOLARD's iPhone is assigned phone number (360) 395-5222, with Apple  
11 ID bradwoolard@ymail.com (**Target Account 1**). Pursuant to the warrant, investigators  
12 searched WOOLARD's iPhone and learned two email accounts were synced with this  
13 iPhone, bradwoolard79@gmail.com (**Target Account 2**) and bradwoolard@ymail.com  
14 (**Target Account 1**). Multiple documents previously seized from WOOLARD's Residence  
15 identified (360) 395-5222 and bradwoolard79@gmail.com (**Target Account 2**) as belonging  
16 to WOOLARD.

17 72. Investigators reviewed email messages stored on WOOLARD's iPhone from  
18 the Gmail account bradwoolard79@gmail.com (**Target Account 2**). Multiple email  
19 messages were observed that appeared to be WOOLARD, using bradwoolard79@gmail.com  
20 (**Target Account 2**), communicating with individuals, apparently in China in order to obtain  
21 various chemical substances, including fentanyl and furanyl fentanyl.

22 73. For example, in March 2016, WOOLARD, using bradwoolard79@gmail.com  
23 (**Target Account 2**), exchanged emails with the user of the email address best-  
24 feel@mail.com. On or about March 20, 2016, WOOLARD received an email from the user  
25 of best-feel@mail.com, stating "Congratulations! Your payment for this order was  
26 confirmed, thanks a lot! We will pack the product well on a secret basis and arrange the  
27 shipping on work day ASAP, if delay for some other reasons, will let you know soon.  
28 Tracking num will be given in 24-48 hours, check your email box then. Best-feel is your

1 honest and reliable supplier! Pleasure to do business with you!..." The next day,  
2 WOOLARD wrote, "I paid the 60\$ shipping. If possible please express mail it. Thank you  
3 very much. You have been a huge help. I plant to be a loyal customer for a long time."  
4 Later that day, the user of best-feel@mail.com wrote to WOOLARD, "hi Brad Woolard. We  
5 have confirmed your payment, thanks a lot! Would arrange the shipping from our American  
6 storage today ASAP, wait for our good news."

7 74. On or about March 26, 2016, WOOLARD wrote, "I need to stock up so I don't  
8 run into this problem of being out of product. What size pkg do u recommend?? I don't want  
9 to loose it in customs. I'm thinking 50g or 100g. What is my price?? And lead time?" The  
10 user of best-feel@mail.com replied, "Don't worry, we always pack well and deliver the  
11 package in our way, very safe and we guaranteed delivery. It could be \$650 for 50g and  
12 \$950 for 100g, both including shipping cost for you. Usually it takes about 6-9 days to  
13 arrive your at door. Btw, you need to offer us a true address, and not to miss the package  
14 again!" Two days later, WOOLARD sent, "I was so excited to see the package in the mail  
15 until I saw this. This is not the product I received last time." The following day WOOLARD  
16 sent, "What is this?? All the Fu-f I've ever gotten from three vendors has been clean white  
17 powder." The user of best-feel@mail.com apologized to WOOLARD and explained the  
18 mistake, "you have gotten in hand must be 5g th-pvp" and then said "your order must have  
19 been sent to our other client by mistake ... maybe we need to reship your order from our  
20 factory in China, how about it?" WOOLARD replied, "shit man I'm scared for the guy who  
21 got my package. He could easily die. It's a very strong chemical u need to track him down  
22 and tell him ASAP. Please overnight from USA if at all possible. I'm way behind."

23 75. Based on my training and experience, and my familiarity with this  
24 investigation, I believe that "Fu-f" is WOOLARD's shorthand for furanyl fentanyl, and that  
25 the prices quoted by best-feel@mail.com are for 50g or 100g of furanyl fentanyl.  
26 Additionally, I believe that WOOLARD told the supplier in China that he has purchased  
27 furanyl fentanyl from three difference suppliers in the past.

1           76. On or about April 1, 2016, WOOLARD, using bradwoolard79@gmail.com  
 2 (Target Account 2), emailed best-feel@mail.com and asked, "I have a Chinese vendor who  
 3 wants to do business with you. Should I introduce you??" In another email that day,  
 4 WOOLARD wrote, "The Chinese vendor wants to buy from u." On or about April 5, 2016,  
 5 the user of best-feel@mail.com wrote back, "Usually, we dont supply our products to the  
 6 competitors, sorry, cant help. Have a good day!"

7           77. On or about June 19, 2016, WOOLARD, using bradwoolard79@gmail.com  
 8 (Target Account 2), again emailed best-feel@mail.com and wrote, "my friend it's been a  
 9 while. Do u still have fu-f?? If so how much for 100g?" The user of best-feel@mail.com  
 10 replied, "hi Brad Woolard, nice to see you again. Yes, we have lots of FU-F in stock, could  
 11 be \$950 for 100g for you, including shipping cost. Have a nice weekend!" WOOLARD  
 12 then asked, "Do u by chance have real fent?? That's what my clients want." The user of  
 13 best-feel@mail.com replied, "sorry brad woolard. It was not legal in China, and nobody  
 14 could supply the real one Have a good day?" WOOLARD replied, "I have a supplier who  
 15 has the real one if you want to purchase from her it is very high-quality." In these email  
 16 messages, investigators believe that WOOLARD was inquiring the price for 100 grams of  
 17 furanyl fentanyl.

18 ***Review of eBay, PayPal, and CBP Records***

19           78. According to records obtained from eBay, WOOLARD had two eBay  
 20 accounts. The first account has user ID "wobra.br.kcmtwxi" (Target Account 6) with the  
 21 full name of "Brad Woolard," the address of 9717 99<sup>th</sup> Ave NE, Arlington, WA, the phone  
 22 number of 360-395-5222 and email address of bradwoolard79@gmail.com (Target  
 23 Account 2). Based on the name, phone number, and address match, investigators believe  
 24 this eBay account is WOOLARD's.

25           79. According to the eBay records, on April 18, 2016, WOOLARD, under his  
 26 user ID "wobra.br.kcmtwxi" (Target Account 5), purchased "the molds "G3722" for tablet  
 27 press pill press die pill maker TDP-0/1.5/5/6." According to an internet search, pills marked  
 28 "G3722" contain Alprazolam which is a schedule IV controlled substance.



1       80. WOOLARD's second eBay account has the user ID "woola-bra" (**Target**  
2 **Account 5**) with the full name of "Brad Woolard," the address of #108 526n west ave,  
3 Arlington, WA 98223, the phone number of 360-395-5222 and email address of  
4 bradwoolard@ymail.com (**Target Account 1**). During the search of the WOOLARD  
5 Residence, investigators found documents with WOOLARD's name and this address. For  
6 example, on July 28, 2018, in the master bedroom closet, investigators found a billing  
7 statement for April 2017 from Washington State Employment Security Department  
8 addressed to "Woolard Contracting LLC," at "108 526 N West Ave, Arlington, WA 98223."  
9 Also, investigators have obtained records from Arlington Copy Mail & More, located at 526  
10 N West Avenue, Arlington, Washington 98223. According to those records, Bradley  
11 WOOLARD rented mailbox 108 at this location on or about December 10, 2008. The  
12 records include copies of WOOLARD's passport and Washington driver's license. Based on  
13 the name, phone, and address match, investigators believe this eBay account is  
14 WOOLARD's.

15       81. In the shipping address history for WOOLARD's eBay account with user ID  
16 "woola-bra", one of the shipping address is listed as Keith STRAND at 1443 Lake Drive,  
17 Camano Island, WA 98282, with a phone number of 360-659-5222 (i.e., the number for  
18 WOOLARD's seized iPhone).

19       82. According to eBay records for WOOLARD's "woola-bra" (**Target Account 5**)  
20 account, in auctions that ran from January 2015 through February and March 2016,  
21 WOOLARD purchased molds for "30M," "A215," "K9," and "X2" for the TDP-0/1.5/5/6  
22 pill presses for \$109, \$109, \$109 and \$119 respectively. As discussed above, the pills seized  
23 from THOMPSON and WOOLARD were marked "M30" and the pills from WOOLARD's  
24 residence tested positive for fentanyl. According to an internet search, pills marked "M30,"  
25 "A215" and "K9" all contain 30 mg of Oxycodone Hydrochloride, and pills marked "X2"  
26 are Xanax, which contains Alprazolam.

27       83. According to eBay records for WOOLARD's "woola-bra" (**Target Account 5**)  
28 account, in an auction that ran from September 2014 through September 16, 2016,

1 WOOLARD purchased item number 191324194073, an “automatic single punch tablet press  
2 pill making machine maker TDP-5 New,” for \$1,619.60 . An internet search shows that the  
3 TDP-5 is a Desktop Tablet Press manufactured by LFA Tablet presses capable of pressing  
4 5400 pills per hour with a listed weight of 125 kg or approximately 275 pounds.

5 84. According to PayPal records, WOOLARD has two separate PayPal accounts in  
6 the name Bradley Woolard with the email address of bradwoolard79@gmail.com (**Target**  
7 **Account 2**). According to PayPal records, on February 8, 2016, WOOLARD sent a payment  
8 of \$1,710.80 to Sanven Corporation for the eBay purchase of item ID 191324194073,  
9 described as an “automatic single punch tablet press pill making machine maker TDP-5  
10 new,” with a listed shipping address of “Keith Strand, 1443 Lake Dr., Camano Island, WA  
11 98282.”

12 85. According to U.S. Customs and Border Protection’s records, a parcel entered  
13 the United States addressed to STRAND at “1443 Lake Dr., Camano Island, WA” from  
14 Shanghai Chengxiang Machinery in China with an arrival date listed as November 11, 2016.  
15 The description of the cargo was “machinery for candy press” and the weight was listed at  
16 716 pounds.

17 86. Additionally, CBP records show that between August 31, 2016 and March 22,  
18 2017, six parcels entered the United States addressed to STRAND at “1443 Lake Dr.,  
19 Camano Island, WA” from Wu Zong Hui at “61 Jianning Road No. 3 building 1502 Room”  
20 with the cargo listed as “sample” and weight between 0.18 kg and 0.23 kg and a listed value  
21 of \$5. As discussed above, investigators seized parcels addressed to BATES and  
22 BERGSTROM, from the same shipper with similar shipping information, and the contents of  
23 these packages tested positive for a fentanyl analogue.

24 87. Based on the information set forth herein, to include these CBP, eBay and  
25 Paypal records, investigators believe that WOOLARD purchased a pill press which he had  
26 shipped to STRAND. Additionally, investigators believe that WOOLARD used this pill  
27 press to manufacture fentanyl-laced, counterfeit Oxycodone pills which he distributed.

1 ***Search of STRAND's residence and interview***

2 88. On October 2, 2018, investigators observed Keith STRAND leave his  
3 residence at 1443 Lake Drive, Camano Island, Washington, and drive away in a Ford Bronco  
4 registered to him at that location. Investigators stopped the Bronco, and STRAND and his  
5 Bronco were transported back to the residence. Investigations then executed a previously  
6 authorized federal search warrant at STRAND's residence. Investigators did not locate any  
7 drugs at STRAND's residence.

8 89. Investigators advised STRAND of his *Miranda* rights, which he indicated he  
9 understood. STRAND agreed to speak with investigators.

10 90. STRAND provided written consent to search his cell phone and his Bronco.  
11 Investigators did not find any drugs in STRAND's Bronco. Investigators did not find any  
12 messages in STRAND's phone that appeared to relate to drugs or money laundering.  
13 Investigators did not find any known phone numbers for WOOLARD stored in STRAND's  
14 contacts.

15 91. During the interview, STRAND stated, among other things, that he has known  
16 WOOLARD for over 20 years and that he currently works for WOOLARD as a contractor.  
17 STRAND stated that he met WOOLARD when they were neighbors and WOOLARD was  
18 living with WOOLARD's parents in Marysville, Washington. STRAND stated that  
19 WOOLARD has a house in the Arlington/Marysville area and that WOOLARD is married  
20 with two children. (Based upon the investigation, I am aware that WOOLARD is married to  
21 Shawna BRUNS, and they have two children.)

22 92. Investigators asked STRAND if WOOLARD had ever been to STRANDS'  
23 house. STRAND stated that WOOLARD "rarely" visits STRAND's house, only a "couple"  
24 of times per year.

25 93. Investigators asked STRAND if WOOLARD had ever asked STRAND to  
26 receive packages at STRAND's house. STRAND said WOOLARD had never asked  
27 STRAND to receive packages.

1 94. Investigators asked STRAND if he had mail taken from his mailbox.  
2 STRAND said there were issues in the past with people stealing mail from the mailbox, but  
3 he now had a locking mailbox. STRAND stated that the mailbox lock was broken for a  
4 period of time, but he repaired that. STRAND stated that sometimes mail is delivered to the  
5 front door, not his mailbox.

6 95. Investigators asked STRAND if he knew what fentanyl was. STRAND stated  
7 that he was aware of fentanyl, but never used it. He stated that he used to grow marijuana  
8 under his house and in his front yard, but that he got rid of it about four or five months ago.

9 96. Investigators asked STRAND about parcels containing fentanyl being shipped  
10 from China to STRAND's house. STRAND denied any knowledge of receiving packages  
11 from China.

12 97. Investigators asked STRAND about receiving a pill press from China that was  
13 ordered by WOOLARD. STRAND denied any knowledge of receiving a pill press from  
14 China.

15 98. Investigators asked STRAND about sending money via Western Union to  
16 China. STRAND denied any knowledge of sending money to China using Western Union.

17 ***Review of Western Union Records***

18 99. Investigators have reviewed documents obtained from Western Union  
19 Financial Services, Inc. that pertain to 2015 through late October 2018. These Western  
20 Union records did not reflect any wire transfers made by WOOLARD during that time  
21 period.

22 100. Notwithstanding STRAND's assertion to investigators that he had never sent  
23 money to China using Western Union, the Western Union records reviewed by investigators  
24 show that STRAND did, in fact, send money to China on multiple occasions. According to  
25 the Western Union records, Keith STRAND, 1443 Lake Drive, Camano Island, Washington,  
26 transferred money to individuals in China, as summarized in the following table. The table  
27 does not include all of the information obtained from Western Union regarding these  
28

transfers, but does show the amount of the wire transfer; the date and time of the transfer; the payee's name; and the payee's destination (address, city, state, and zip code), in China:

US Dollars Sent	Send Date	Send Time (EST)	Payee Full Name Provided by Payee	Street Address Provided by Payee	Address City Provided by Payee	Address State Code Provided by Payee	Address Zip Code Provided by Payee
900.00	7/18/2017	16:06:00	FENGJUN HUANG	CHANGJIANGLU	HEFEI	AN	230000
900.00	7/17/2017	17:42:00	FENGJUN HUANG	CHANGJIANGLU	HEFEI	AN	230000
900.00	7/17/2017	17:40:00	FENGJUN HUANG	CHANGJIANGLU	HEFEI	AN	230000
1800.00	3/11/2017	13:08:00	JIEMEI LOU	GUICHILU	HEFEI	AN	230000
1800.00	3/11/2017	12:59:00	JIEMEI LOU	GUICHILU	HEFEI	AN	230000
1800.00	1/12/2017	17:59:00	FENGJUN HUANG	CHANGJIANGLU	HEFEI	AN	230000
1800.00	1/12/2017	17:45:00	FENGJUN HUANG	CHANGJIANGLU	HEFEI	AN	230000
1500.00	4/4/2016	18:33:00	XULONG ZHUANG	DADIANZHEN XUEJIAYAOCUN 711HAO	JUNANXIAN	Sh	102218

101. The Western Union records for the April 4, 2016, January 12, 2017, and March 11, 2017, transactions reflect STRAND's date of birth and his Washington driver's license number, which are consistent with records from the Washington Department of Licensing. The Western Union records do not reflect STRAND's date of birth or driver's license number for the July 17 and 18, 2017 transfers.

102. According to the Western Union records, STRAND sent the July 17 and 18, 2017 wires from Rite Aid, 26817 88<sup>th</sup> Avenue NW, Stanwood, Washington; the January 12,



1 2017, and March 11, 2017 wires from QFC, 27008 92<sup>nd</sup> Avenue NW, Stanwood,  
 2 Washington; and the April 4, 2016 wire from Fred Meyer, 12906 Bothell Everett Highway,  
 3 Everett, Washington.

4 103. Additionally, the Western Union tracking number (MTCN) for the July 17,  
 5 2017, transaction at 17:42:00 was 3920127463. This is the same MTCN as that on the  
 6 Western Union receipt found in WOOLARD's master bedroom closet on July 28, 2018. In  
 7 other words, WOOLARD had the receipt for this particular transaction.

8 ***Service Provider Records for Target Accounts 1 and 2***

9 104. On or about November 12, 2018, investigators received records from Google.  
 10 According to those records, bradwoolard79@gmail.com (**Target Account 2**), is a Gmail  
 11 email address used by Brad WOOLARD with a Google Account ID of 205674908021. The  
 12 Google records also list a "SMS" as +13603955222 (the number for WOOLARD's seized  
 13 iPhone, discussed herein) and indicate the account was created on February 21, 2014. The  
 14 listed recovery email is bradwoolard@ymail.com (**Target Account 1**). Google records  
 15 indicated that this account has access to the following services: Android, Chromeos Login,  
 16 Gmail, Google Calendar, Google Chrome Sync, Google Cloud Print, Google Docs, Google  
 17 Drive, Google Hangouts, Google Maps Engine, Google My Maps, Google Payments, Google  
 18 Photos, Google Play Music, Google+, Has Google Profile, Has Plusone, Location History,  
 19 Web & App Activity, and YouTube. As discussed elsewhere in this affidavit, the listed  
 20 email addresses and phone number are believed to be used by WOOLARD. According to  
 21 the records from Google, the last logins to bradwoolard79@gmail.com (**Target Account 2**)  
 22 occurred on or about August 28, 2018, July 21, 2018, and June 21, 2018 (twice). According  
 23 to the Google records, the IP address associated with the June 21, 2018 logins is  
 24 50.34.172.105.

25 105. On or about December 10, 2018, investigators received records from Oath  
 26 Holdings, Inc. (formerly Yahoo Holdings Inc.). According to those records, "Mr Brad  
 27 Woolard", who resided in the United States, in zip/postal code 98223, created the email  
 28 account bradwoolard@ymail.com (**Target Account 1**) on August 12, 2008. The records

also indicate that that an alternate communication channel for WOOLARD was “3603955222” (the number for WOOLARD’s seized iPhone, discussed herein). The records indicate that the properties used on this account were Flickr and Mail. Flickr is an image and video hosting service that is owned by Oath Holdings, Inc (formerly Yahoo Holdings Inc). Flickr allows registered users to upload and share photos and videos. Users can access their Flickr account using apps on various platforms, iOS, Windows, Mac, Android, etc. According to these records, the most recent logins to bradwoolard@ymail.com (**Target Account 1**) took place on July 28, 2018, and June 21, 2018 (three times). The IP address associated with the June 21, 2018 logins is also 50.34.172.105.

106. On October 16, 2018 and January 31, 2019, DEA sent preservation letters to Oath Holdings for **Target Account 1**. On September 6, 2018 and January 31, 2019, DEA sent a preservation letter to Google for **Target Account 2**.

#### ***Search of WOOLARD’s iCloud Account***

107. On November 27, 2018, investigators received records from Apple. According to the Apple records, an Apple account with Apple ID bradwoolard@ymail.com (**Target Account 1**) in the name of Brad WOOLARD at 9717 99<sup>th</sup> Ave Northeast Arlington, Washington with a full iCloud backup. The day phone number associated to this account is 360-395-5222. These records show that this Apple account was created on April 10, 2013. The records also show an iTunes subscriber signup date of September 18, 2009. As discussed above, the information for Apple ID bradwoolard@ymail.com (**Target Account 1**) matches the information that investigators have for WOOLARD.

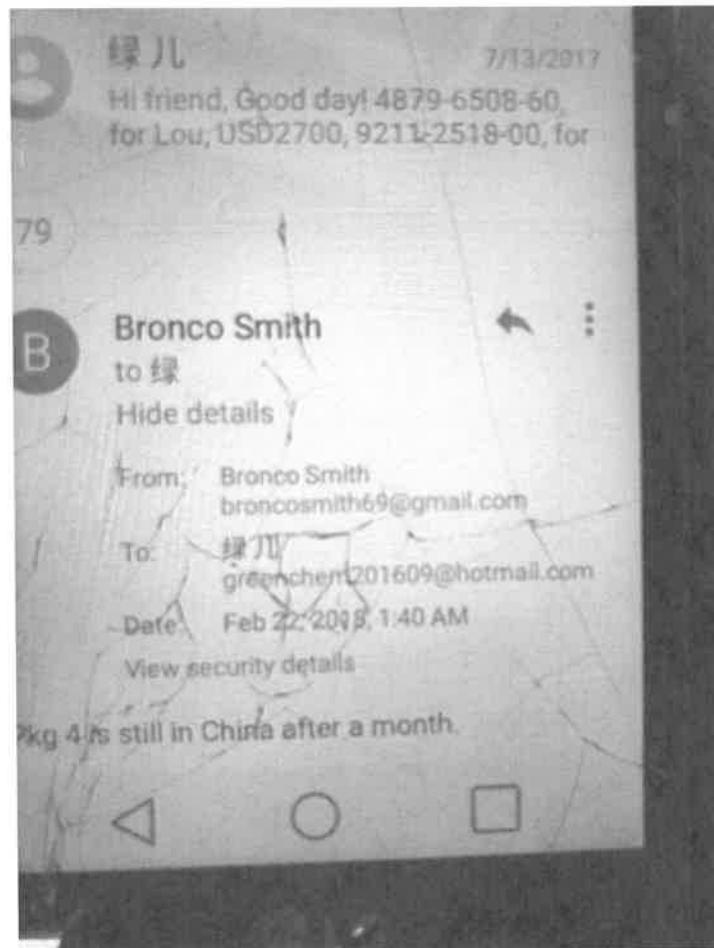
108. On January 22, 2019, US Magistrate Judge Paula L. McCandlis signed a search warrant for multiple Apple iCloud accounts, including bradwoolard@ymail.com. On the same date, investigators electronically served the search warrant on Apple. On February 6, 2019, investigators received records from Apple in response to the search warrant.

109. During a review of the records provided by Apple in response to this search warrant, investigators determined that most of the records had been encrypted and were not

1 accessible to investigators. However, investigators were able to view WOOLARD's contact  
2 list and photographs.

3 110. During a review of the photos provided by Apple for the account with Apple  
4 ID bradwoolard@ymail.com (**Target Account 1**), in the name Brad WOOLARD,  
5 investigators identified four photos (which I will refer to as Photographs #1 – 4) that show  
6 email messages displayed on the screen of a cell phone. Although the sender and recipient  
7 email addresses are visible in only one of these photos, investigators believe all of the email  
8 exchanges pertain to wire transfers of funds to China to pay for fentanyl, for the reasons  
9 discussed below.

10 111. A copy of a photograph that I will refer to "Photograph #1" is set forth below:



112. According to the metadata for Photograph #1, this photograph was taken on February 23, 2018, at 1:19 p.m. using an iPhone 7 and the GPS Location was recorded as 48.08425, -122.09675. According to Google Maps, these GPS coordinates are at the WOOLARD Residence.

113. Photograph #1 depicts an email message chain with the first message dated “7/13/2017” and the visible text as “Hi friend, Good day 4879-6508-60, for Lou, USD2700, 92112518-00, for” followed by 79 messages which are compressed and not visible. Almost seven months later, an email dated February 22, 2018, at 1:40 a.m., the user of the email account broncosmith69@gmail.com (**Target Account 4**) sent an email to greenchem201609@hotmail.com (**Target Account 3**), stating, “Pkg 4 is still in China after a month.”

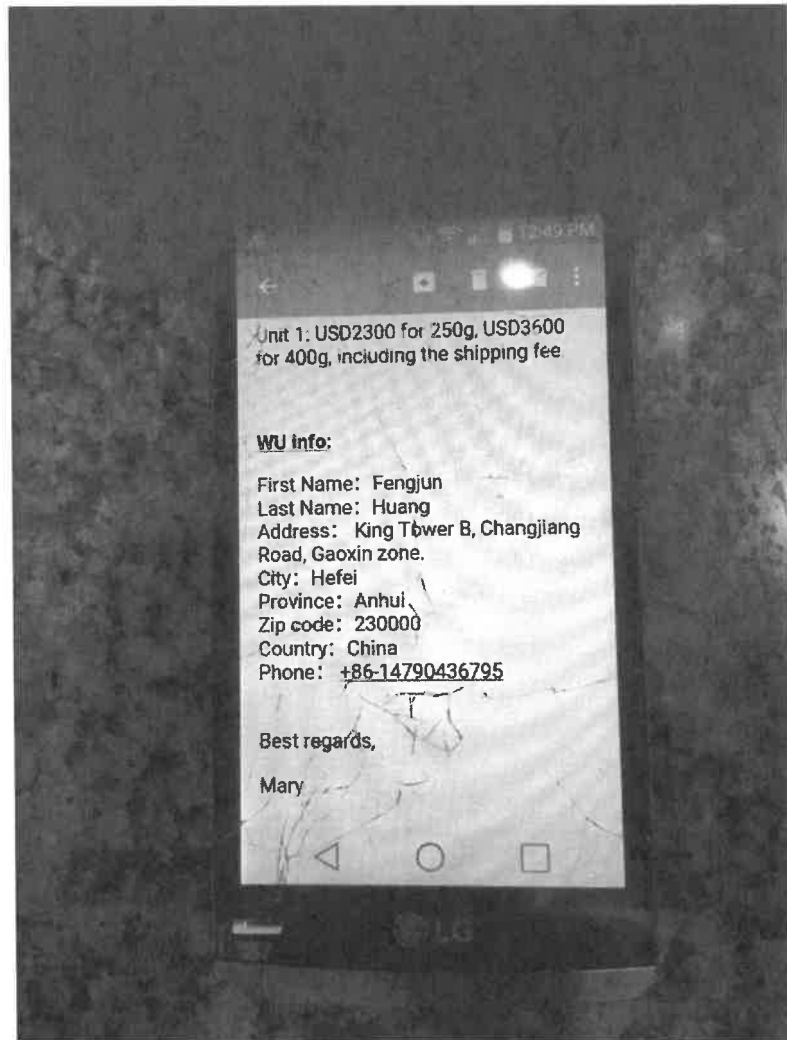
114. Based on my training and experience, I know that Western Union tracking numbers (MTCN) are ten digits long.<sup>4</sup> As such, investigators believe that the ten-digit numbers in this email could be MTCNs, particularly as the email also states “USD 2700,” which likely refers to \$2,700 in U.S. Dollars.

115. Based upon my familiarity with this investigation, to include the shipment of fentanyl and its analogues from China, prices for fentanyl and its analogues, and WOOLARD’s involvement in distribution of fentanyl-laced counterfeit oxycodone pills, I believe that when broncosmith69@gmail.com (**Target Account 4**), wrote, “Pkg 4 is still in China after a month,” I believe that the user of broncosmith69@gmail.com (**Target Account 4**) was referring to a previously ordered package of controlled substances and was stating that said package was still located in China.

116. A copy of a photograph that I will refer to as Photograph #2 is set forth below:

---

<sup>4</sup> The ten-digit numbers depicted in Photograph #1 do not match the MTCNs for the wire transfers that STRAND is known to have made to China based upon the Western Union records provided.



117. According to the metadata for Photograph #2, this photograph was taken on January 11, 2017, at 12:49 p.m., using an iPhone 6s and the GPS Location was recorded as 48.0844, -122.09703. According to Google Maps, these GPS coordinates are at the WOOLARD Residence.

118. I was present at the execution of search warrants at the WOOLARD Residence, and I have also reviewed photographs taken during the search of the WOOLARD Residence. The granite in the background of Photograph #2 appears to be similar to, if not the same as, the granite in the kitchen at the WOOLARD Residence.

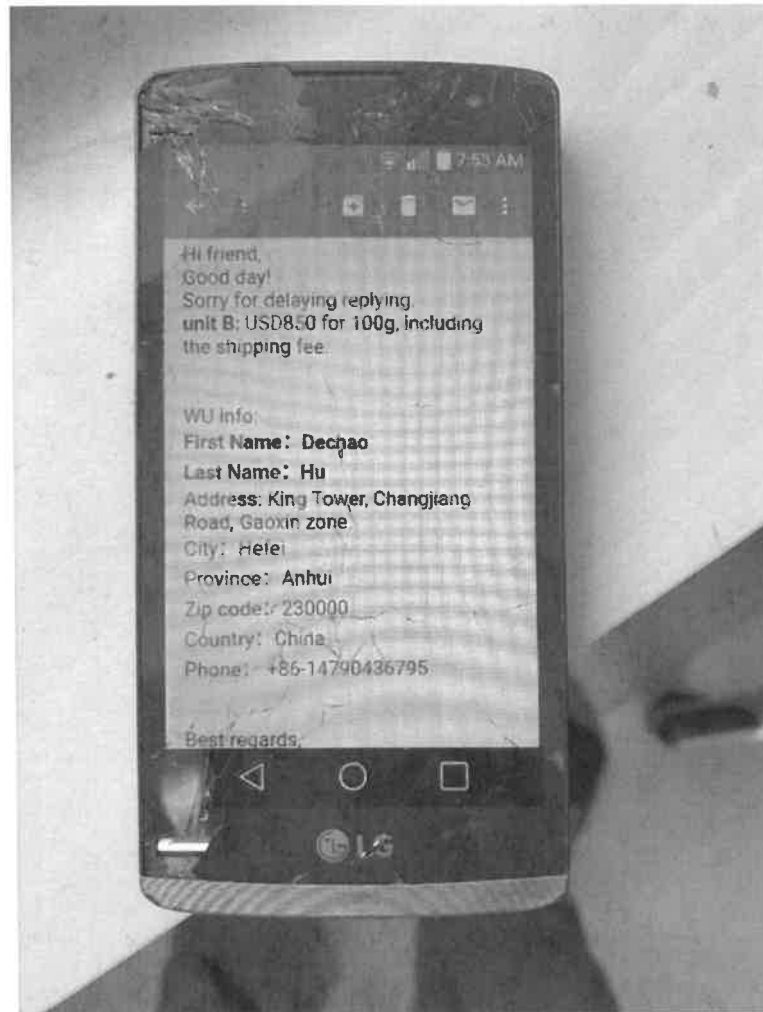


119. A copy of a photograph that I will refer to as Photograph #3 is set forth below:



120. According to the metadata for Photograph #3, this photograph was taken on March 4, 2017, at 8:23 a.m., using an iPhone 6s and the GPS Location was recorded as 48.08416, -122.09708. According to Google Maps, these GPS coordinates are at the WOOLARD Residence.

121. A copy of a photograph that I will refer to as Photograph #4 is set forth below:



122. According to the metadata for Photograph #4, this photograph was taken on June 6, 2018, at 7:53 a.m., using an iPhone 7 and the GPS Location was recorded as 48.06612, -122.10303. According to Google Maps, this location is approximately 1.5 miles from the WOOLARD Residence.

123. The dates, sender email address(es), and recipient email address(es) are not visible in Photographs 2-4. However, in light of the commonalities between the messages in Photographs 1-4 and the circumstances of this investigation, investigators believe that all four photographs pertain to payments of funds to China for purchase of fentanyl and/or its analogues.

124. In reviewing Photographs #1-4, investigators noticed many similarities in the emails, in addition to the similar formatting. In particular, Photographs #1 and 3 each refer to “Lou”; Photographs #2 and 3 are each from “Mary”; Photographs #1, 3 and 4 each begin, “Hi friend [...] Good day!”; and Photographs #2, 3, and 4 each include “WU Info,” which investigators believe refers to a payee, payee address, and payee phone number, to be used in conjunction with wiring funds via Western Union.

125. The payee names in Photographs # 2-4 differ. The payee in Photograph #2 is “Fengjun Huang”, which is the same payee in the Western Union receipt found in WOOLARD’s bedroom closet. Per Western Union records, STRAND transferred money via Western Union on five separate occasions to “Fengjun Huang” in China. The payee in Photograph #3 is “Jiemei Lou.” Per Western Union records, STRAND transferred money via Western Union on two separate occasions to “Jiemei Lou.”

126. Although the payee names in Photographs #2-4 differ, the payee telephone number is the same in each photograph.<sup>5</sup> Also, each payee address includes Changjiang City, Heifei, Anhui, 230000.

127. Photographs #1, 2, and 4 refer to “USD” (which commonly refers to U.S. Dollars). Photographs #2 and 4 appear to refer to prices in dollars that includes a “shipping fee.” Specifically, Photograph #2 states, in part, “Unit 1: USD2300 for 250g, USD3600 for 400g, including the shipping fee.” Photograph #4 states, in part, “Unit B: USD850 for 100g, including the shipping fee.”

128. As discussed above, in the emails between WOOLARD (using **Target Account 2**) and best-feel@mail.com, WOOLARD was quoted a price of \$650 for 50 grams of furanyl fentanyl and \$950 for 100 grams of furanyl fentanyl. The prices stated in Photographs #2 and 4 are broadly consistent with the prices quoted in the best-feel@mail.com emails. Thus, in light of the investigation to date, investigators suspect that

---

<sup>5</sup> The phone number reflected in Photographs #2-4 does not match the payee phone numbers for STRAND’s known wire transfers to China.

1 greenchem201609@hotmail.com (**Target Account 3**) is quoting prices for fentanyl, furanyl  
2 fentanyl, or another fentanyl analogue.

3 ***Service Provider Records for Target Account 3***

4 129. On or about March 8, 2019, investigators received records received from  
5 Microsoft. According to those records, greenchem201609@hotmail.com (**Target**  
6 **Account 3**) is registered in the name “儿 绿” and the country listed as China with no  
7 address, city, or state. According to Google Translate, 儿 translates into “child” and 绿  
8 translates into “green.” Additionally, the service used for **Target Account 3** is Mail.  
9 **Target Account 3** was created on September 23, 2016 and was last accessed on  
10 February 15, 2019. On March 26, 2019, DEA sent a preservation letter to Microsoft for  
11 greenchem201609@hotmail.com (**Target Account 3**).  
12

13 ***Search of WOOLARD’s iPad Mini***

14 130. Investigators have begun their review of the data recovered from the iPad  
15 seized from the WOOLARD Residence. The “Owner Name” is listed as “Brad’s iPad” and  
16 the associated Apple ID is bradwoolard@ymail.com (**Target Account 1**). As discussed  
17 above, this is WOOLARD’s known Apple ID. Investigators located numerous photos stored  
18 in this device which depict WOOLARD and BRUNS. Investigators noticed multiple  
19 references to Craigslist in the browsing history.<sup>6</sup> Multiples photos were found that are  
20 similar to the photos described above from WOOLARD’s iCloud account.

21 131. Investigators reviewed iMessages between bradwoolard@ymail.com (**Target**  
22 **Account 1**) and 1-425-404-1227, which is saved under the contact name “Tonny.” On  
23 January 31, 2017, WOOLARD sent “I have huge respect for you bro. U do good for your  
24 family. Work out stay healthy. I look up to u in a way. I will be more like you. I’m having  
25 a pretty rough time but it’s good. I’m so mad at drugs. I’ll never touch one again. Never  
26

27  
28 <sup>6</sup> Craigslist is a website that lists classified advertisements with sections devoted to jobs, housing, for sale, items wanted, services, etc.

1 give me any. Ever. Plase no matter what I say or do.” Tonny replied, “Ya I got u bro the first  
 2 week is gonna b rough u can get threw it and leaving for a month after is the smartest thing u  
 3 can do that will help out a lot and once u get there won’t be nothing around and u just gotta  
 4 focus on stacking money plus this time ur not gonna be hurting for cash U can keep urself  
 5 busy and not b worried about bills being paid u kno.” Based on these messages and the  
 6 messages discussed below, investigators believe that WOOLARD is referring to not using  
 7 drugs any longer, not stopping his distribution activities

8 132. The following exchange between WOOLARD and “tonny” occurred on  
 9 February 7, 2017:

10 WOOLARD: “Tim said the things were bad. I’ll call him in a he to see how.”

11 WOOLARD: “A hr”

12 WOOLARD: “U will have to make adjustments”

13 Tonny: “Ok just let me kno cuz those r the ones me and u made”

14 WOOLARD: “Really?? They should be fine”

15 Tonny: “Ya, I haven’t gave him any yet the last ones he got were from u”

16 WOOLARD: I guess the strength is down a bit and not quite hard enuf. Both will be  
 17 fixed by increasing the weight. Please weigh them and if you can break them with  
 18 your fingers they are to soft. Moving the machine did this I’m sure.”

19 Tonny: “I was about to over there to work what should I do”

20 Tonny: “Ya I was weighing the ones I made made sure they’re were 128 right”

21 WOOLARD: “We might have to add a lil active to it. We will have to grind and  
 22 repress when I get back but for now we just fix and make more. They should weigh  
 23 I’ll know more later just hang tight for now.”

24 WOOLARD: “Pull the dry pads out that might be affecting it”

25 WOOLARD: “Fuck”

26 Tonny: “Ok”

27 Tonny: “I moved almost 2k so far and no one has called me I wonder why they  
 28 calling him that’s weird”



1 WOOLARD: "I'll do some math and u can add like .02 mg to each on before next  
2 press. They have bigger tolerances."

3 WOOLARD: "He has fiends"

4 WOOLARD: "I'll hit u back later"

5 Tonny: "Ok should I go take those pads out real quick"

6 Tonny: "Or just wait for ur call"

7 WOOLARD: "I'm doing some math. Give me a min"

8 WOOLARD: "Ok weigh out 1560g of mix. Add 2.5g of active that has been ground.

9 Mix super good. That will make close to 12000 for his next batch. Make them . 130 ea  
10 but same size. Should fix it."

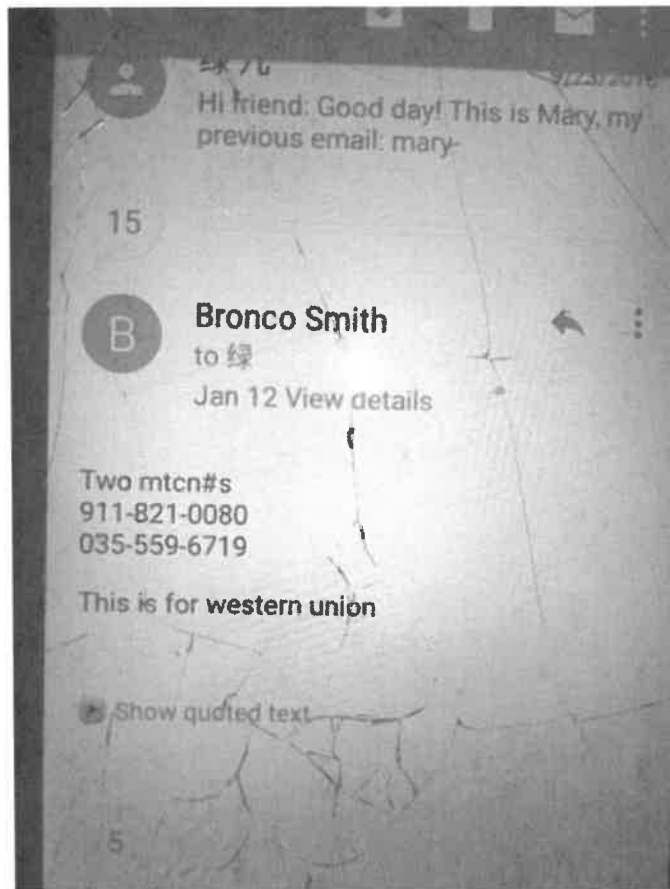
11 133. In the messages described above, investigators believe that "Tonny" told  
12 WOOLARD that their customer "Tim" complained about the potency of the pills.

13 Investigators believe that the term "active," as used by WOOLARD is a reference to the  
14 active ingredient in the pills, believed to be fentanyl or a fentanyl analogue. Investigators  
15 believe that WOOLARD and "Tonny" discussed how to increase the potency of the pills that  
16 "Tonny" was pressing on WOOLARD's behalf in response to "Tim's" complaint about  
17 potency. The message exchange concluded with WOOLARD providing "Tonny" with an  
18 updated "recipe" for the pills.

19 134. Investigators also reviewed iMessages between bradwoolard@ymail.com  
20 (**Target Account 1**) and "Shawna Marie," using phone number 425-501-9209. Investigators  
21 identified a message dated January 29, 2017, from "Shawna Marie," which said "Kisses miss  
22 you tons. How are you doing" with a photo of BRUNS attached. Based on my participation  
23 in this investigation, I am familiar with BRUNS' appearance, and I believe that "Shawna  
24 Marie" is Shawna Marie BRUNS, WOOLARD's wife.

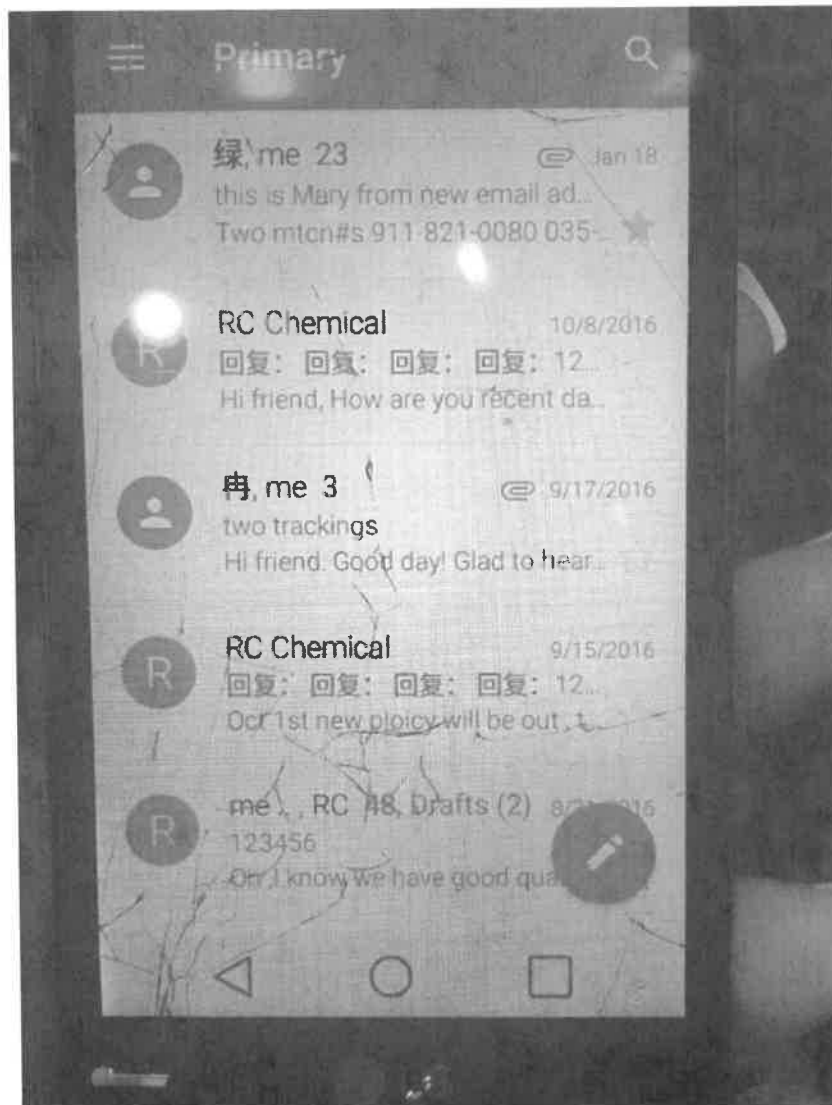
25 135. On January 30, 2017, WOOLARD wrote, "I'm going to gym. Can u send me a  
26 pic of the tracking #s from email on my other phone. U might have to dig a bit to find them."  
27 WOOLARD and BRUNS then exchanged multiple messages until BRUNS asked "Who is  
28 the email from Mary or Rc chem." WOOLARD replied, "Marry it is resent" and "Newest

1 email w tracking # on pictures.” BRUNS responded by sending the following photograph,  
 2 which I will refer to as Photograph #5, and wrote, “That it?”:



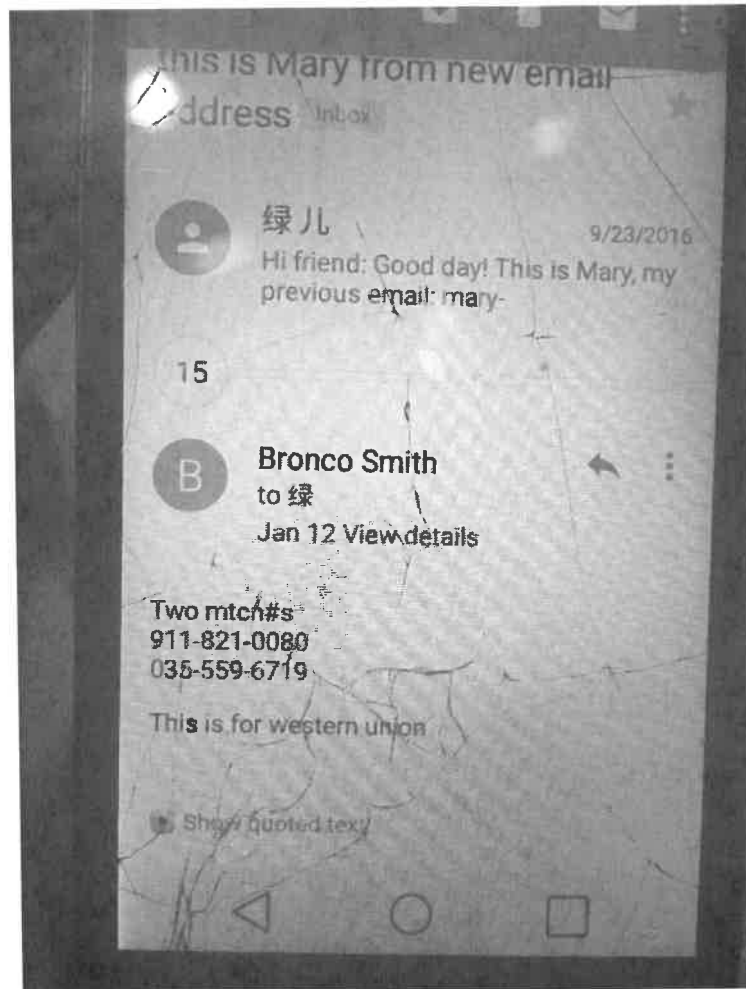
136. The MTCN numbers listed in Photograph #5 -- 911-821-0080 and 035-559-6719 – match the MTCN numbers for STRAND’s two wire transfers on January 12, 2017, to Fengjun HUANG. The metadata indicates that Photograph #5 was taken on January 29, 2017, at 4:47 p.m., using an iPhone 6s with no location data present.

137. WOOLARD replied, “Close” and “Pictures of packages and mail labels.” BRUNS and WOOLARD exchanged multiple emails where they discussed where to find the emails WOOLARD was looking for. BRUNS then sent the following photograph, which I will refer to as Photograph #6:



138. WOOLARD and BRUNS continued to exchange messages with WOOLARD directing BRUNS where to find the emails. During that exchange, BRUNS sent the photographs discussed below to WOOLARD.

139. BRUNS sent WOOLARD a photograph that I will refer to as Photograph #6, which is set forth below. Photograph #6 appears to depict the same email shown in Photograph #5:

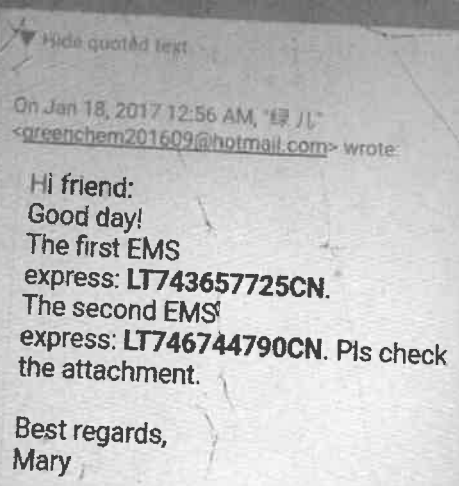


140. Next, BRUNS sent WOOLARD a photograph that I will refer to as Photograph #7, which is set forth below:

//

//

//



- 发件人: 绿儿 – Sender: Green Child
- 发送时间: 2017年 1 月16日 1:51:00 – Sending time: 2017 year 1 month 16 day 1:51:00
- 收件人: Bronco Smith – Recipient: Bronco Smith
- 主题: 答复(repeating) – Theme: reply (repeating)

Affidavit of SA Cheng / 47  
USAO No. 2018R00949



143. Next, BRUNS sent WOOLARD a photograph, which I will refer to as Photograph #8, and wrote, "That was under it too." Photograph #8 is set forth below:



144. After receiving Photograph #8 from BRUNS, WOOLARD replied, "Thank you. You rock."

145. Investigators believe that in these messages BRUNS sent WOOLARD photographs of emails that WOOLARD had saved on a different phone. Photograph #7 includes an email from greenchem201609@hotmail.com (**Target Account 3**) dated January 18, 2017, and refers to "EMS Express." According to a Google search, EMS Express is an international express postal service. Based upon my participation in this

1 investigation, I believe that in this email exchange, “Mary” (the user of **Target Account 3**)  
2 was providing “Bronco Smith” with two tracking numbers for packages mailed from China  
3 that contained fentanyl (or its analogues).

4 146. I also note that in Photograph #5, the Chinese character, which translates to  
5 green” in the “To” line, is the same as in Photograph #1 and in the subscriber information for  
6 greenchem201609@hotmail.com (**Target Account 3**). The emails depicted in Photograph  
7 #1 and #5 both appear to originate from “Bronco Smith.” Additionally, Photographs #7 and  
8 #8 are from “Mary,” similar to Photographs #2 and #3.

9 147. In light of the above, investigators believe that WOOLARD is the user of the  
10 broncosmith69@gmail.com (**Target Account 4**).

11 ***Service Provider Records for Target Account 4***

12 148. On or about March 18, 2019, investigators received records from Google.  
13 According to those records, broncosmith69@gmail.com (**Target Account 4**) is a Gmail  
14 email address in the name of “Bronco Smith” with Account ID 886914477346 which was  
15 created on April 4, 2016 with the last logins dated June 6, 2018, March 21, 2018 and  
16 December 19, 2017. The listed “SMS” is 425-239-1748. Google records indicated that this  
17 account has access to the following services: Android, Gmail, Google Calendar, Google  
18 Chrome Sync, Google Hangouts, Location History, Minutemaid, Web & App Activity and  
19 YouTube.

20 149. Investigators search the Washington Department of Licensing and did not find  
21 any driver’s licenses or vehicles registered to “Bronco Smith,” as such, investigators believe  
22 that “Bronco Smith” is a fictitious name.

23 150. According to AT&T, 425-239-1748 was activated on April 4, 2016, and was  
24 subscribed to Tracfone at 8390 Northwest 25<sup>th</sup> Street, Doral, Florida. This phone was active  
25 until May 8, 2017. Investigators have requested subscriber information from Tracfone and  
26 are waiting for results.

1 ***Status of the Case***

2 151. On September 1, 2018, WOOLARD was arrested as he attempted to enter the  
3 United States using his U.S. Passport at the San Ysidro port of entry.<sup>7</sup>

4 152. On September 13, 2018, a federal grand jury in the Western District of  
5 Washington returned an Indictment charging WOOLARD and THOMPSON in *United States*  
6 *v. Woolard, et al.*, CR18-217RSM, with *Conspiracy to Distribute Controlled Substances*, in  
7 violation of 21 U.S.C. §§ 841(a)(1), 841(b)(1)(A) and 846 (Count 1), and *Possession of*  
8 *Furanyl Fentanyl with Intent to Distribute*, in violation of 21 U.S.C. §§ 841(a)(1) and  
9 841(b)(1)(A) and 18 U.S.C. § 2 (Count 2). WOOLARD was also charged with *Possession of*  
10 *Furanyl Fentanyl with Intent to Distribute*, in violation of 21 U.S.C. §§ 841(a)(1) and  
11 841(b)(1)(A) and 18 U.S.C. § 2 (Count 3), *Felon in Possession of Firearms*, in violation of  
12 18 U.S.C. § 922(g)(1) (Count 4), and *Possession of Firearms in Furtherance of a Drug*  
13 *Trafficking Offense*, in violation of 18 U.S.C. § 924(c).<sup>8</sup>

14 153. On September 13, 2018, THOMPSON was arrested pursuant to an arrest  
15 warrant.<sup>9</sup>

16 154. Trial in this matter is scheduled for July 15, 2019.

17 **B. Knowledge Based On Training and Experience**

18 155. Based on my training and experience, and my discussions with other  
19 experienced officers and agents involved in drug investigations, I know the following:

20 a. Traffickers of controlled substances, and those who assist them,  
21 maintain and tend to retain accounts or records of their drug trafficking activities, including  
22 lists of drug quantities and money owed, telephone records including contact names and  
23 numbers, photographs, and similar records of evidentiary value. These items are generally

24  
25 <sup>7</sup> WOOLARD has remained in custody since his arrest on September 1, 2018.

26 <sup>8</sup> WOOLARD was previously convicted of a crime punishable by imprisonment for a term exceeding  
27 one year, to wit: Use of a Building for Unlawful Drugs, on or about September 24, 2004, in Island  
28 County Superior Court., Case No. 04-1-00050-6.

<sup>9</sup> Following a detention hearing on September 19, 2018, the Court released THOMPSON and placed  
him on pretrial supervision.

1 kept in locations where drug traffickers believe their property is secure and will remain  
2 undetected from law enforcement, such as inside their homes, vehicles and storage lockers.

3           b.       Traffickers of controlled substances commonly maintain addresses,  
4 vehicles, or telephone numbers which reflect names, addresses, vehicles, and/or telephone  
5 numbers of their suppliers, customers and associates in the trafficking organization and it is  
6 common to find drug traffickers keeping records of said associates in cellular telephones and  
7 other electronic devices. Traffickers almost always maintain cellular telephones for ready  
8 access to their clientele and to maintain their ongoing narcotics business.

9           c.       Traffickers maintain evidence of their criminal activity at locations that  
10 are convenient to them, including their residences vehicles, and storage lockers. This  
11 evidence often includes more than contraband and paraphernalia and includes financial  
12 records, records of property and vehicle ownership, records of property rented, records of  
13 post office boxes used to ship and receive contraband and currency, records of other storage  
14 facilities used to hide drugs or currency, and other documentary evidence relating to  
15 commission of, and proceeds from, their crimes.

16           d.       During the execution of search warrants, it is common to find papers,  
17 letters, billings, documents, and other writings which show ownership, dominion, and control  
18 of vehicles, residences, and/or storage units.

19           e.       Persons trafficking and using controlled substances commonly sell or  
20 use more than one type of controlled substance at any one time.

21           f.       Traffickers frequently maintain items necessary for weighing,  
22 packaging, and cutting drugs for distribution. This paraphernalia often includes, but is not  
23 limited to, scales, plastic bags, pill presses and cutting/diluting agents and items to mask the  
24 odor of drugs

25           g.       Traffickers often maintain weapons, including guns and ammunition, in  
26 secure locations such as their residences and storage lockers, in order to protect their drugs  
27 and drug proceeds.

1 h. Traffickers often have false identification documents and identification  
2 documents in the names of others.

3 i. Drug trafficking is a cash business, and in order to escape notice from  
4 authorities for using unexplained income, or hide excessive cash from illegal activities,  
5 traffickers either keep large quantities of cash at home or other secure locations such as a  
6 vehicles and storage locker, or convert the cash into other valuable assets, such as jewelry,  
7 precious metals, monetary instruments, or other negotiable forms of wealth. Records of such  
8 conversions are often stored where a trafficker lives.

9 156. A pill press or encapsulating machine, and its associated equipment, are used to  
10 convert powder drugs to pill form. I know that a pill press or encapsulating machine is a  
11 device used to convert powdered drugs, from a powdered state to a pill form. I know pill  
12 presses often use casts or dyes that impart a code or stamp on the pill to identify the pill and  
13 its contents. I know that drug traffickers often use dyes that stamp popular or name brand  
14 drug stamps on to imitation drugs, possibly containing fentanyl, to imitate legitimate  
15 narcotics that are then redistributed to other drug traffickers.

16 157. Drug dealers use cellular telephones as a tool or instrumentality in committing  
17 their criminal activity. They use them to maintain contact with their suppliers, distributors,  
18 and customers. They prefer cellular telephones because, first, they can be purchased without  
19 the location and personal information that land lines require. Second, they can be easily  
20 carried to permit the user maximum flexibility in meeting associates, avoiding police  
21 surveillance, and traveling to obtain or distribute drugs. Third, they can be passed between  
22 members of a drug conspiracy to allow substitution when one member leaves the area  
23 temporarily. I also know that it is common for drug traffickers to retain in their possession  
24 phones that they previously used, but have discontinued actively using, for their drug  
25 trafficking business. Based on my training and experience, the data maintained in a cellular  
26 telephone used by a drug dealer is evidence of a crime or crimes. This includes the  
27 following:



1           a.       The assigned number to the cellular telephone (known as the mobile  
2 directory number or MDN), and the identifying telephone serial number (Electronic Serial  
3 Number, or ESN), (Mobile Identification Number, or MIN), (International Mobile  
4 Subscriber Identity, or IMSI), or (International Mobile Equipment Identity, or IMEI) are  
5 important evidence because they reveal the service provider, allow us to obtain subscriber  
6 information, and uniquely identify the telephone. This information can be used to obtain toll  
7 records, to identify contacts by this telephone with other cellular telephones used by co-  
8 conspirators, to identify other telephones used by the same subscriber or purchased as part of  
9 a package, and to confirm if the telephone was contacted by a cooperating source or was  
10 intercepted on a wiretap here or in another district.

11           b.       The stored list of recent received calls and sent calls is important  
12 evidence. It identifies telephones recently in contact with the telephone user. This is valuable  
13 information in a drug investigation because it will identify telephones used by other  
14 members of the organization, such as suppliers, distributors, and customers, and it confirms  
15 the date and time of contacts. If the user is under surveillance, it identifies what number he  
16 called during or around the time of a drug transaction or surveilled meeting. Even if a contact  
17 involves a telephone user not part of the conspiracy, the information is helpful (and thus is  
18 evidence) because it leads to friends and associates of the user who can identify the user,  
19 help locate the user, and provide information about the user. Identifying a defendant's law-  
20 abiding friends is often just as useful as identifying his drug-trafficking associates.

21           c.       Stored text messages and stored emails are important evidence, similar  
22 to stored numbers. Agents can identify both drug associates, and friends of the user who  
23 likely have helpful information about the user, his location, and his activities.

24           d.       Photographs on a cellular telephone are evidence because they help  
25 identify the user, either through his or her own picture, or through pictures of friends, family,  
26 and associates that can identify the user. Pictures also identify associates likely to be  
27 members of the drug trafficking organization. Some drug dealers photograph groups of  
28 associates, sometimes posing with weapons and showing identifiable gang signs.

1 e. Stored address records are important evidence because they show the  
2 user's close associates and family members, and they contain names and nicknames  
3 connected to phone numbers that can be used to identify suspects.

4 f. It is common for drug traffickers to use encrypted means of  
5 communication, such as WhatsApp, Signal, Wickr, and Telegram, to attempt to avoid  
6 detection by law enforcement. It is common for drug traffickers to install and use these apps  
7 on their phones in order to make encrypted calls and send encrypted messages.

8 158. Based on my training and experience, and my discussions with other  
9 experienced officers and agents involved in drug investigations, I also know that drug  
10 traffickers ordering fentanyl (or fentanyl analogues) from sources of supply based in China  
11 often search for these sources of supply through internet searches and online marketplaces. I  
12 also know that drug traffickers often pay for these drugs using means such as international  
13 wire transfers (*e.g.*, money transfers made via Western Union or other money service  
14 businesses) and through use of cryptocurrency (also referred to as digital or virtual currency)  
15 such as Bitcoin.

16 159. Additionally, investigators believe that WOOLARD and his criminal  
17 associates have used pill presses locally to convert the white fentanyl powder into counterfeit  
18 light blue M30s. Notwithstanding the execution of multiple search warrants in this  
19 investigation, investigators have not yet located or seized the pill press (or pill presses) used  
20 by WOOLARD and his coconspirators.

## 21 **VII. BACKGROUND REGARDING ONLINE SERVICES**

22 160. Based on my training and experience, and information from other experienced  
23 agents, I know the following information:

24 161. As explained herein, information stored in connection with an online account  
25 may provide crucial evidence of the "who, what, why, when, where, and how" of the  
26 criminal conduct under investigation, thus enabling the United States to establish and prove  
27 each element or alternatively, to exclude the innocent from further suspicion.

1 162. The information stored in connection with an online account can indicate who  
2 has used or controlled the account. This “user attribution” evidence is analogous to the  
3 search for “indicia of occupancy” while executing a search warrant at a residence. For  
4 example, email communications, contacts lists, and images sent (and the data associated with  
5 the foregoing, such as date and time) may indicate who used or controlled the account at a  
6 relevant time.

7 163. Further, information maintained by the email provider can show how and when  
8 the account was accessed or used. For example, as described below, email providers  
9 typically log the Internet Protocol (IP) addresses from which users access the email account,  
10 along with the time and date of that access. By determining the physical location associated  
11 with the logged IP addresses, investigators can understand the chronological and geographic  
12 context of the email account access and use relating to the crime under investigation. This  
13 geographic and timeline information may tend to either inculcate or exculpate the account  
14 owner. Additionally, information stored at the user's account may further indicate the  
15 geographic location of the account user at a particular time (e.g., location information  
16 integrated into an image or video sent via email).

17 164. Stored electronic data may provide relevant insight into the email account  
18 owner's state of mind as it relates to the offense under investigation. For example,  
19 information in the email account may indicate the owner's motive and intent to commit a  
20 crime (e.g., communications relating to the crime), or consciousness of guilt (e.g., deleting  
21 communications in an effort to conceal them from law enforcement).

22 **A. Background Regarding Yahoo's services**

23 165. As discussed above, Yahoo is the Service Provider for **Target Account 1**.  
24 Based on my training and experience, and information from other experienced agents, I  
25 know the following information regarding Yahoo's services:

26 166. Yahoo provides a variety of on-line services, including electronic mail  
27 (“e-mail”) access, to the general public. Yahoo allows subscribers to obtain e-mail accounts  
28 at the domain names yahoo.com and ymail.com.

***Subscriber Records and E-mail Content***

167. Subscribers obtain an account by registering with Yahoo. When doing so, Yahoo asks the subscriber to provide certain personal identifying information. This information can include the subscriber's full name, physical address, telephone numbers and other identifiers, alternative e-mail addresses, and, for paying subscribers, means and source of payment (including any credit or bank account number). In my training and experience, such information may constitute evidence of the crimes under investigation because the information can be used to identify the account's user or users, to help establish who has dominion and control over the account, and to help identify other accounts that are used by same account user or users.

168. E-mail providers typically retain certain transactional information about the creation and use of each account on their systems. This information can include the date on which the account was created, the length of service, records of log-in (i.e., session) times and durations, the types of service utilized, the status of the account (including whether the account is inactive or closed), the methods used to connect to the account (such as logging into the account via Yahoo), and other log files that reflect usage of the account. In addition, e-mail providers often have records of the Internet Protocol address ("IP address") used to register the account and the IP addresses associated with particular logins to the account. Because every device that connects to the Internet must use an IP address, IP address information can help to identify which computers or other devices were used to access the e-mail account, which can help establish the individual or individuals who had dominion and control over the account

169. In general, an e-mail that is sent to a Yahoo subscriber is stored in the subscriber's "mail box" on Yahoo's servers until the subscriber deletes the e-mail. If the subscriber does not delete the message, the message can remain on Yahoo's servers indefinitely. Even if the subscriber deletes the e-mail, it may continue to be available on Yahoo's servers for a certain period.

1 170. When the subscriber sends an e-mail, it is initiated at the user's computer,  
2 transferred via the Internet to Yahoo's servers, and then transmitted to its end destination.  
3 Yahoo often maintains a copy of the e-mail sent. Unless the sender of the e-mail specifically  
4 deletes the e-mail from the Yahoo server, the e-mail can remain on the system indefinitely.  
5 Even if the sender deletes the e-mail, it may continue to be available on Yahoo's servers for  
6 a certain period.

7 171. A sent or received e-mail typically includes the content of the message, source  
8 and destination addresses, the date and time at which the e-mail was sent, and the size and  
9 length of the e-mail. If an e-mail user writes a draft message but does not send it, that  
10 message may also be saved by Yahoo but may not include all of these categories of data.

11 172. Account activity may provide relevant insight into the account owner's state of  
12 mind as it relates to the offenses under investigation. For example, information on the  
13 account may indicate the owner's motive and intent to commit a crime (e.g., information  
14 indicating a plan to commit a crime), or consciousness of guilt (e.g., deleting account  
15 information in an effort to conceal evidence from law enforcement).

16 ***Other Content***

17 173. A Yahoo subscriber can also store files, including address books, contact or  
18 buddy lists, calendar data, photographs, documents and other files, on servers maintained  
19 and/or owned by Yahoo. In my training and experience, evidence of who was using an  
20 account may be found in these other files stored in relation to the account. For example,  
21 photographs stored in relation to an online account may contain photographs of the account  
22 user, documents stored in relation to the account may include references to the account user,  
23 contact lists and calendar data may reveal information that identifies the account user as well  
24 as co-conspirators.

25 174. I know based on my training and experience and my review of Yahoo's  
26 services, that Yahoo provides users with access to an address book in which they may store  
27 contact information including names, addresses, e-mail address, and telephone numbers.  
28 Yahoo also provides users access to a "Calendar" file that may include notes of events and



schedules. Yahoo also provides users with access to a service called “Flicker” that can be used to create photo albums, store photographs, and share photographs with others. Yahoo also provides users with access to Yahoo Groups which allows users to share photographs, calendars and messages with others who typically share a common interest.

#### ***Yahoo Location Records***

175. Yahoo also collects certain location information related to Yahoo account holders. On Yahoo’s webpage under “Yahoo Privacy Policy,” Yahoo informs users that it may collect account holders’ location information such as:

- **Pinpointed Physical Location**

If you provide permission through your device, browser, or with Yahoo directly, Yahoo may obtain pinpointed physical location information from technologies like GPS, Wi-Fi, or cell tower proximity.

- **Locations You Entered**

- Yahoo may collect locations that you searched for in certain properties (such as Search and Maps).

- Locations added by you through the Location Settings page are also collected by Yahoo.

- You may be asked to provide a location such as postal code. Yahoo may use this information to provide a starting point for location-aware products and services.

- **IP Address**

- Yahoo may use your IP address to derive information about where your device is generally located. Please refer to IP Address for more information.

- **Partner Location Information**

- Yahoo may work with select partners to obtain location information about some of our registered users. . . .

- Yahoo may receive location data from third parties that you have linked your account with. You can view, manage, add, or removed Linked Accounts.

176. Yahoo further informs its account holders that it “may access, store, and use the location information described above to provide services such as: enhanced location based services, serve location-targeted advertising, search results, and other content. Yahoo may maintain a history of your locations. . . . Other uses of location information may include determining the appropriate language for presenting a website, conducting product analysis, and assisting in the detection of fraud and abuse.”

177. Yahoo account holders may be able to withdraw location collection permission on their devices by opting out. According to Yahoo, it obtains account holders’ consent (an opt-in) before using information from pinpointing technology such as GPS and cell tower information. Yahoo allows users to withdraw consent (opt-out) for the use of such information by Yahoo. Yahoo informs users that it may use and store this information, in combination with other location-based information such as IP address, billing postal code provided by the account holders’ carrier or registration location, to provide enhanced location based services, serve location-targeted advertising, search results, and other content. In addition, users can choose to make their current location data available to third party widget developers by giving Yahoo permission to share the data.

178. Based on the above, I know that if the users of the target Yahoo email accounts utilize a mobile device to access these Yahoo accounts and have not disabled location services on their device/s or through their Yahoo account settings, Yahoo may have detailed records of the locations at which the account holders utilized their mobile devices. This type of evidence may further assist in identifying the account holders, and lead to the discovery of other evidence of the crimes under investigation.

#### ***Customer Service Communications***

179. In some cases, e-mail account users will communicate directly with an e-mail service provider about issues relating to the account, such as technical problems, billing

1 inquiries, or complaints from other users. E-mail providers typically retain records about  
 2 such communications, including records of contacts between the user and the provider's  
 3 support services, as well records of any actions taken by the provider or user as a result of  
 4 the communications. In my training and experience, such information may constitute  
 5 evidence of the crimes under investigation because the information can be used to identify  
 6 the account's user or users.

7 **B. Background Regarding Google's Services**

8 180. As discussed above, Google is the Service Provider for **Target Account 2** and  
 9 **Target Account 4**. Based on my training and experience, and information from other  
 10 experienced agents, I know the following information regarding Google services:

11 181. Google provides a variety of on-line services, including electronic mail  
 12 ("e-mail") access and instant messaging (otherwise known as "chat" messaging), to the  
 13 general public. Google provides subscribers e-mail and chat accounts at the domain name  
 14 "@gmail.com." Google also allows subscribers to register a custom domain name and set up  
 15 Google services such as chat and e-mail using that domain name instead of "@gmail.com."

16 ***Subscriber Records and Account Content***

17 182. Subscribers obtain an account by registering with Google. When doing so,  
 18 e-mail providers like Google ask the subscriber to provide certain personal identifying  
 19 information. This information can include the subscriber's full name, physical address,  
 20 telephone numbers and other identifiers, alternative e-mail addresses, and, for paying  
 21 subscribers, means and source of payment (including any credit or bank account number). In  
 22 my training and experience, such information may constitute evidence of the crimes under  
 23 investigation because the information can be used to identify the account's user or users, and  
 24 to help establish who has dominion and control over the account.

25 183. E-mail providers typically retain certain transactional information about the  
 26 creation and use of each account on their systems. This information can include the date on  
 27 which the account was created, the length of service, records of log-in (i.e., session) times  
 28 and durations, the types of service utilized, the status of the account (including whether the

1 account is inactive or closed), the methods used to connect to the account (such as logging  
2 into the account via Google's websites), and other log files that reflect usage of the account.  
3 In addition, e-mail providers often have records of the Internet Protocol address ("IP  
4 address") used to register the account and the IP addresses associated with particular logins  
5 to the account. Because every device that connects to the Internet must use an IP address, IP  
6 address information can help to identify which computers or other devices were used to  
7 access the e-mail account.

8 184. In some cases, e-mail account users will communicate directly with an e-mail  
9 service provider about issues relating to the account, such as technical problems, billing  
10 inquiries, or complaints from other users. E-mail providers typically retain records about  
11 such communications, including records of contacts between the user and the provider's  
12 support services, as well records of any actions taken by the provider or user as a result of  
13 the communications. In my training and experience, such information may constitute  
14 evidence of the crimes under investigation, because the information can be used to identify  
15 the account's user or users.

16 185. In general, an e-mail that is sent to a Google subscriber is stored in the  
17 subscriber's "mail box" on Google's servers until the subscriber deletes the e-mail. When  
18 the subscriber sends an e-mail, it is initiated at the user's computer, transferred via the  
19 Internet to Google servers, and then transmitted to its end destination. Google often  
20 maintains a copy of received and sent e-mails. Unless the sender specifically deletes an e-  
21 mail from the Google server, the e-mail can remain on the system indefinitely. Even if the  
22 subscriber deletes the e-mail, it may continue to be available on Google's servers for some  
23 period of time.

24 186. A sent or received e-mail typically includes the content of the message, source  
25 and destination addresses, the date and time at which the e-mail was sent, and the size and  
26 length of the e-mail. If an e-mail user writes a draft message but does not send it, that  
27 message may also be saved by Google but may not include all of these categories of data.  
28

1 187. In addition to e-mail and chat, Google offers subscribers numerous other  
2 services including: Android, Blogger, Google Alerts, Google Calendar, Google Chrome  
3 Sync, Google Cloud Print, G-Suite, Google Developers Console, Google Drive, Google  
4 Hangouts, Google Maps, Google Payments, Google Photos, Google Search Console, Google  
5 Voice, Google+, Google Profile, Location History, Web & Activity, and YouTube, among  
6 others. Thus, a subscriber to a Google account can also store files, including address books,  
7 contact lists, calendar data, photographs and other files, on servers maintained and/or owned  
8 by Google. For example, Google Calendar is a calendar service that users may utilize to  
9 organize their schedule and share events with others. Google Drive may be used to store  
10 data and documents, including spreadsheets, written documents (such as Word or Word  
11 Perfect) and other documents that could be used to manage a website. Google Photos can be  
12 used to create photo albums, store photographs, and share photographs with others and "You  
13 Tube," allows users to view, store and share videos. Google Search Console records a  
14 Google account user's search queries. Google Web & Activity records certain browsing  
15 history depending on whether the account holder is logged into their account. Like many  
16 internet service companies, the services Google offers are constantly changing and evolving.

17 188. Based upon my training and experience, all of these types of information may  
18 be evidence of crimes under investigation. Stored e-mails and chats not only may contain  
19 communications relating to crimes, but also help identify the participants in those crimes.  
20 For example, address books and contact lists may help identify and locate co-conspirators.  
21 Similarly, photographs and videos of co-conspirators may help identify their true identities,  
22 as opposed to supposed identities that they have used in telephone or e-mail  
23 communications. Documents such as Google sheets may identify the scope of the criminal  
24 activity. Calendar data may reveal the timing and extent of criminal activity. Search and  
25 browsing history can also be extremely useful in identifying those using anonymous online  
26 accounts and may also constitute direct evidence of the crimes under investigation to the  
27 extent the browsing history or search history might include searches and browsing history  
28 related to drug distribution over the internet, obtaining fentanyl and its analogues from



1 China, money laundering, and other evidence of the crimes under investigation or indications  
2 of the true identity of the account users.

3 189. Google is also able to provide information that will assist law enforcement in  
4 identifying other accounts associated with the Google Target Account, namely, information  
5 identifying and relating to other accounts used by the same subscriber. This information  
6 includes any forwarding or fetching accounts<sup>10</sup> relating to the Target Account, all other  
7 Google accounts linked to the Target Account because they were accessed from the same  
8 computer (referred to as “cookie overlap”), all other Google accounts that list the same SMS  
9 phone number as the Target Account, all other Google accounts that list the same recovery  
10 e-mail addresses<sup>11</sup> as do the Target Account, and all other Google accounts that share the  
11 same creation IP address as the Target Account. Information associated with these  
12 associated accounts will assist law enforcement in determining who controls the Target  
13 Account and will also help to identify other e-mail accounts and individuals relevant to the  
14 investigation.

#### 15 ***Google Location History and Location Reporting***

16 190. According to Google’s website, “Location Reporting” allows Google to  
17 periodically store and use a device’s most recent location data in connection with the Google  
18 Account connected to the device. “Location History” allows Google to store a history of  
19 location data from all devices where a user is logged into their Google Account and have  
20 enabled Location Reporting. According to Google “[w]hen you turn on Location Reporting  
21 for a device like your iPhone or iPad, it lets Google periodically store and use that device’s  
22 most recent location data in connection with your Google Account.” How often Location  
23 Reporting updates location data is not fixed. Frequency is determined by factors such as how

---

24  
25 <sup>10</sup> A forwarding or fetching account related to a Target Account would be a separate e-mail account  
26 that can be setup by the user to receive copies of all of the e-mail sent to the Target Account.

27 <sup>11</sup> The recovery e-mail address is an additional e-mail address supplied by the user that is used by  
28 Google to confirm the username after the user creates an e-mail account, help the user if the user has  
trouble signing into the user’s Google account or has forgotten the user’s password, or alert the user  
to any unusual activity involving user’s Google e-mail address.

1 much battery life the device has, if the device is moving, or how fast the device is moving.  
2 Google's location services may use GPS, Wi-Fi hotspots, and cellular network towers to  
3 determine an account holder's location.

4 191. Based on the above, I know that if a user of a gmail email account utilizes a  
5 mobile device to access that account and has not disabled location services on his or her  
6 device/s or through the Google account settings, Google may have detailed records of the  
7 locations at which the account holders utilized the mobile device/s. This type of evidence  
8 may further assist in identifying the account holders, and lead to the discovery of other  
9 evidence of the crimes under investigation.

10 192. I know that Google's Android service collects and stores identifying  
11 information about an Android smart phone used to access the Google account, including the  
12 International Mobile Equipment Identifier (IMEI), International Mobile Subscriber Identity  
13 (IMSI), telephone number and mobile carrier code. I know that Google's Location History  
14 service periodically queries the physical location of a device that is currently accessing a  
15 Google account through the device's GPS, nearby Wi-Fi network IDs and cellular tower  
16 information and records a history of device movements in Google's servers.

17 **C. Background Regarding Microsoft's Services**

18 193. As discussed above, Microsoft is the Service Provider for **Target Account 4**.  
19 Based on my training and experience, and information from other experienced agents, I  
20 know the following information regarding Microsoft's services:

21 194. Microsoft is an internet service provider that offers a variety of online services  
22 including email accounts (Outlook.com or Hotmail), cloud computing (Microsoft OneDrive,  
23 Office and Office365), gaming services (Xbox), video conferencing (Skype), web browsing  
24 and search tools (Bing Search, Microsoft Edge, and Internet Explorer), maps, an online  
25 marketplace (Microsoft Store), and other services. Microsoft also provides remote  
26 computing services for devices that use Windows operating systems, including security  
27 services and parental control services which collect information about the use of the devices  
28 (e.g., internet browsing history, software usage history, and other information).

1 195. A Microsoft account (formerly known as a Windows Live account) is what  
2 Microsoft customers may use to sign into Microsoft services such as Outlook.com (or  
3 Hotmail), Office, OneDrive, Skype, Xbox, Windows, and more. A user may create a  
4 Microsoft account with any email address (Microsoft accounts are not limited to those who  
5 use Microsoft email accounts) and a password and thereafter use that email address and  
6 password to sign in to any Microsoft program or service.

7 196. In my training and experience email providers like Microsoft typically retain  
8 certain transactional information about the creation and use of each account on their systems.  
9 This information can include the date on which the account was created, the length of  
10 service, records of log-in (i.e., session) times and durations, the types of service utilized, the  
11 status of the account (including whether the account is inactive or closed), the methods used  
12 to connect to the account (such as logging into the account via a website), and other log files  
13 that reflect usage of the account. In addition, email providers often have records of the IP  
14 address used to register the account and the IP addresses associated with particular logins to  
15 the account. Because every device that connects to the Internet must use an IP address, IP  
16 address information can help to identify which computers or other devices were used to  
17 access the email account, which can help establish the individual or individuals who had  
18 dominion and control over the account

19 197. In general, an email that is sent to a Microsoft subscriber is stored in the  
20 subscriber's "mail box" on Microsoft's servers until the subscriber deletes the email. If the  
21 subscriber does not delete the message, the message can remain on Microsoft's servers  
22 indefinitely. Even if the subscriber deletes the email, it may continue to be available on  
23 Microsoft's servers for a certain period of time.

24 198. When the subscriber sends an email, it is initiated at the user's computer,  
25 transferred via the Internet to Microsoft's servers, and then transmitted to its end destination.  
26 Microsoft often maintains a copy of the email sent. Unless the sender of the email  
27 specifically deletes the email from Microsoft's server, the email can remain on the system  
28

1 indefinitely. Even if the sender deletes the email, it may continue to be available on  
2 Microsoft's servers for a certain period of time.

3 199. A sent or received email typically includes the content of the message, source  
4 and destination addresses, the date and time at which the email was sent, and the size and  
5 length of the email. If an email user writes a draft message but does not send it, that message  
6 may also be saved by Microsoft but may not include all of these categories of data.

7 200. Microsoft provides a variety of online, or "cloud," services in addition to email  
8 access, to the public and to customers who utilize Hotmail accounts that are served by  
9 Microsoft. Microsoft's various cloud services are associated with a single Microsoft  
10 account, which is typically associated with a Microsoft email address, but can be associated  
11 with any email address. The various cloud services provided by Microsoft are optional and  
12 can be turned "on" or "off" by the user.

13 201. In providing services such as Outlook, OneDrive, Xbox, calendar services,  
14 online file storage, storage of browsing history, storage of search history, and locations  
15 history, Microsoft collects information that constitute evidence of the crimes under  
16 investigation. For example, such evidence can be used to discover or confirm the identity  
17 and location users of the service at a particular time.

#### 18 **D. Background Regarding eBay's Services**

19 202. As discussed above, I know that eBay is the Service Provider for **Target**  
20 **Account 5** and **Target Account 6**. Based on my training and experience, I have learned the  
21 following about eBay and communications between its customers:

22 203. eBay is an Internet consumer-to-consumer corporation, headquartered in San  
23 Jose, California. The company manages eBay.com, an online auction and shopping website  
24 in which people and businesses buy and sell a broad variety of goods and services  
25 worldwide. eBay is considered an electronic communications service ("ECS") provider  
26 because it provides its users access to electronic communications service as defined in  
27 Title 18, United States Code, Section 2510(15). eBay users have access for these electronic  
28 communication services, also known as "member to member" communications, by

1 registering an account with eBay. eBay requests subscribers to provide basic information,  
2 such as name, gender, zip code and other personal/biographical information. However, eBay  
3 does not verify the information provided.

4 204. eBay maintains electronic records pertaining to the individuals and companies  
5 for which they maintain user accounts. These records include account access information,  
6 e-mail transaction information, and account application information.

7 205. Subscribers to eBay may access their accounts on servers maintained or owned  
8 by eBay from any computer connected to the Internet located anywhere in the world.

9 206. Any "member to member" e-mail that is sent to an eBay user is stored in the  
10 subscriber's "mail box" on eBay's servers until the subscriber deletes the e-mail or the  
11 subscriber's mailbox exceeds the storage limits preset by the internet service provider. If the  
12 message is not deleted by the subscriber, the account is below the storage limit, and the  
13 subscriber accesses the account periodically, that message can remain on eBay's servers until  
14 they are archived after a period of six months.

15 207. When the subscriber sends a "member to member" e-mail, it is initiated at the  
16 user's computer, transferred via the Internet to eBay's servers, and then transmitted to its end  
17 destination. eBay users have the option of saving a copy of the e-mail sent. Unless the  
18 sender of the e-mail specifically deletes the e-mail from the eBay server, the e-mail can  
19 remain on the system and are archived after six months. The sender can delete the stored  
20 e-mail message, thereby eliminating it from the e-mail box maintained at eBay, but that  
21 message will remain in the recipient's e-mail box unless the recipient also deletes it or unless  
22 the recipient's account has exceeded its storage limitations.

23 208. An eBay subscriber can store files, including e-mails and image files, on  
24 servers maintained and/or owned by eBay.

25 209. E-mails and image files stored on an eBay server by a subscriber may not  
26 necessarily also be located in the subscriber's home computer. The subscriber may store e-  
27 mails and/or other files on the eBay server for which there is insufficient storage space in the  
28 subscriber's own computer or which the subscriber does not wish to maintain in his or her



1 own computer. A search of the subscriber's home, business, or laptop computer will  
2 therefore not necessarily uncover files the subscriber has stored on the eBay servers.

3 **VIII. INFORMATION TO BE SEARCHED AND THINGS TO BE SEIZED**

4 210. Pursuant to Title 18, United States Code, Section 2703(g), this application and  
5 affidavit for a search warrant seeks authorization to require the Service Providers, and its  
6 agents and employees, to assist agents in the execution of this warrant. Once issued, the  
7 search warrant will be presented to the Service Provider with direction that it identify the  
8 accounts described in Attachments A-1, A-2, A-3 and A-4 to this affidavit, as well as other  
9 subscriber and log records associated with the accounts, as set forth in Section I of  
10 Attachments B-1, B-2, B-3 and B-4 to this affidavit.

11 211. The search warrants will direct the Service Providers to create an exact copy of  
12 the specified accounts and records, including an exact copy of the contents of the hard disk  
13 drive or drives installed on the server associated with the **Target Accounts**, or the original  
14 drives.

15 212. I, and/or other law enforcement personnel will thereafter review the copy of  
16 the electronically stored data, and identify from among that content those items that come  
17 within the items identified in Section II to Attachments B-1, B-2, B-3, and B-4 for seizure.

18 213. Analyzing the data contained in the forensic image may require special  
19 technical skills, equipment, and software. It could also be very time-consuming. Searching  
20 by keywords, for example, can yield thousands of "hits," each of which must then be  
21 reviewed in context by the examiner to determine whether the data is within the scope of the  
22 warrant. Merely finding a relevant "hit" does not end the review process. Keywords used  
23 originally need to be modified continuously, based on interim results. Certain file formats,  
24 moreover, do not lend themselves to keyword searches, as keywords, search text, and many  
25 common e-mail, database and spreadsheet applications do not store data as searchable text.  
26 The data may be saved, instead, in proprietary non-text format. And, as the volume of  
27 storage allotted by service providers increases, the time it takes to properly analyze  
28 recovered data increases, as well. Consistent with the foregoing, searching the recovered

1 data for the information subject to seizure pursuant to this warrant may require a range of  
 2 data analysis techniques and may take weeks or even months. All forensic analysis of the  
 3 data will employ only those search protocols and methodologies reasonably designed to  
 4 identify and seize the items identified in Section II of Attachment B to the warrant.

### 5 IX. CONCLUSION

6 214. Based on the information set forth herein, there is probable cause to search  
 7 **Target Account 1, Target Account 2, Target Account 4, Target Account 5, and Target**  
 8 **Account 6** as further described herein and in Attachments A-1, A-2, and A-4, for evidence,  
 9 fruits and instrumentalities, as further described in Attachments B-1, B-2, and B-4, of crimes  
 10 committed by WOOLARD and his coconspirators, specifically *Distribution of, and*  
 11 *Possession with Intent to Distribute, Controlled Substances*, in violation of Title 21, United  
 12 States Code, Section 841(a)(1); *Conspiracy to Distribute Controlled Substances*, in violation  
 13 of Title 21, United States Code, Sections 841(a)(1) and 846, *Money Laundering*, in violation  
 14 of Title 18, United States Code Section 1956, *Felon in Possession of a Firearm*, in violation  
 15 of Title 18, United States Code, Section 922(g), and *Distribution of controlled substances by*  
 16 *means of the internet*, in violation of Title 21, United States Code, Sections 823, 841(h)(1),  
 17 841(b)(1) and 846.

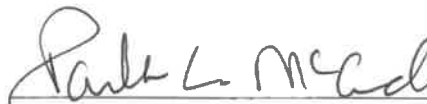
18 215. Based on the information set forth herein, there is probable cause to search  
 19 **Target Account 3** as further described herein and in Attachments A-3, for evidence, fruits  
 20 and instrumentalities, as further described in Attachments B-3, of crimes committed by the  
 21 user (or users) of **Target Account 3**, and their criminal associates, including but not limited  
 22 to WOOLARD, specifically, *Distribution of, and Possession with Intent to Distribute,*  
 23 *Controlled Substances*, in violation of Title 21, United States Code, Section 841(a)(1);  
 24 *Conspiracy to Distribute Controlled Substances*, in violation of Title 21, United States Code,  
 25 Sections 841(a)(1) and 846, *Money Laundering*, in violation of Title 18, United States Code  
 26 Section 1956, and *Distribution of controlled substances by means of the internet*, in violation  
 27 of Title 21, United States Code, Sections 823, 841(h)(1), 841(b)(1) and 846.

1        216. Because the warrants will be served on the Service Providers, who will then  
2 compile the requested records at a time convenient to it, reasonable cause exists to permit the  
3 execution of the requested search warrants at any time in the day or night.

4        217. I further request that the Court order that all papers in support of this  
5 application, including the affidavit and search warrant, be sealed. These documents discuss  
6 an ongoing criminal investigation that is neither public nor known to all of the targets of the  
7 investigation. Accordingly, there is good cause to seal these documents because their  
8 premature disclosure may seriously jeopardize that investigation.

9  
10  
11   
12 JOSEPH CHENG  
13 Special Agent  
14 Drug Enforcement Administration  
15

16        The above-named agent provided a sworn statement attesting to the truth of the  
17 contents of the foregoing affidavit on the 26<sup>th</sup> day of March, 2019.

18   
19  
20 HON. PAULA L. MCCANDLIS  
21 United States Magistrate Judge  
22  
23  
24  
25  
26  
27  
28

**ATTACHMENT A-1**

**Oath Holdings (Yahoo) Accounts to be Searched**

The electronically stored data, information and communications contained in, related to, and associated with, including all preserved data, associated with the following accounts, that are stored at premises controlled by Oath Holdings Inc., formerly Yahoo Holdings, Inc. (“Yahoo”), a company located in Sunnyvale, California:

**bradwoolard@ymail.com (“Target Account 1”)**

**ATTACHMENT B-1****Items to Be Seized (Oath Holdings Inc.)****I. Section I - Information to be disclosed by Oath Holdings Inc. (Yahoo) for search:**

To the extent that the information described in Attachment A-1 is within the possession, custody, or control of Oath Holdings Inc., formerly known as Yahoo Holdings, Inc. ("Yahoo"), regardless of whether such information is located within or outside of the United States, including any e-mails, records, files, logs, or information that has been deleted but is still available to Yahoo, or has been preserved pursuant to a request made under 18 U.S.C. § 2703(f) (please refer to preservation request numbers 391868 and 403025) Yahoo is required to disclose the following information to the government for each of the Target Accounts listed in Attachment A-1, from account inception to the present:

a. The contents of all e-mails associated with the account, including stored or preserved copies of e-mails sent to and from the account, draft e-mails, the source and destination addresses associated with each e-mail, the date and time at which each e-mail was sent, and the size and length of each e-mail;

b. All subscriber records associated with the specified account, including 1) names, email addresses, and screen names; 2) physical addresses; 3) records of session times and durations; 4) length of service (including start date) and types of services utilized; 5) telephone or instrument number or other subscriber number or identity, including any temporarily assigned network address such as internet protocol address, media access card addresses, or any other unique device identifiers recorded by Yahoo in relation to the account; 6) account log files (login IP address, account activation IP address, and IP address history); 7) detailed billing records/logs; 8) means and source of payment; and 9) lists of all related accounts;

c. Any contact lists;

d. Any Yahoo Chat/Messenger information and/or records, including any Yahoo Chat/Messenger Friends list, time, date, and IP address logs for Chat and Messenger use, and any archived web messenger communications stored on Yahoo servers;



- e. Any Yahoo Notepad information and/or records;
- f. Any Yahoo Calendar information and/or records;
- g. Any Yahoo Groups information and/or records including member lists, e-mail addresses of members, messages, files, calendars, database content, and photographs;
- h. Any web search or browsing records;
- i. Any stored documents;
- j. Any Flickr content including Flickr e-mail, photographs and user comments, IP address and timestamp of content uploaded to account;
- k. All GPS, Wi-Fi, or cell tower proximity records related to the account and/or account contents;
- l. Account history, including any records of communications between Yahoo, and any other person about issues relating to the accounts, such as technical problems, billing inquiries, or complaints from other users about the specified account. This to include records of contacts between the subscriber and the provider's support services, as well as records of any actions taken by the provider or subscriber in connection with the service;
- m. All records or other information regarding the identification of the account, to include full name, physical address, telephone numbers and other identifiers, records of session times and durations, the date on which the account was created, the length of service, the IP address used to register the account, log-in IP addresses associated with session times and dates, account status, alternative e-mail addresses provided during registration, methods of connecting, log files, and means and source of payment (including any credit or bank account number);
- n. The types of service utilized;
- o. All records or other information stored at any time by an individual using the account, including address books, contact and buddy lists, calendar data, pictures, and files;

1 p. All records pertaining to communications between the Provider and any  
 2 person regarding the account, including contacts with support services and records of actions  
 3 taken.

4  
 5 Yahoo is hereby ordered to disclose the above information to the government within  
 6 **14 days** of service of this warrant.

7  
 8 **II. Information to be seized by the government**

9 All information described above in Section I that constitutes fruits, contraband,  
 10 evidence and instrumentalities of violations of *Distribution of, and Possession with Intent to*  
 11 *Distribute, Controlled Substances*, in violation of Title 21, United States Code, Section  
 12 841(a)(1); *Conspiracy to Distribute Controlled Substances*, in violation of Title 21, United  
 13 States Code, Sections 841(a)(1) and 846, *Money Laundering*, in violation of Title 18, United  
 14 States Code Section 1956, *Felon in Possession of a Firearm*, in violation of Title 18, United  
 15 States Code, Section 922(g), and *Distribution of controlled substances by means of the*  
 16 *internet*, in violation of Title 21, United States Code, Sections 823, 841(h)(1), 841(b)(1) and  
 17 846, those violations occurring during the period from approximately January 1, 2013 to the  
 18 present, for the Target Account listed on Attachment A-1, including the following:

19 a. Evidence that may identify any coconspirators, aiders and abettors, drug  
 20 suppliers and/or drug customers, including evidence that helps reveal their whereabouts and  
 21 including evidence of relationship(s) that existed prior to January 1, 2013.

22 b. Communications between coconspirators, sources of supply, customers,  
 23 and aiders and abettors regarding the above-referenced crimes and communications in  
 24 furtherance of the above-referenced crimes.

25 c. Evidence regarding the acquisition, importation, transportation,  
 26 shipment, mailing, processing, and distribution of controlled substances.

27 d. Evidence regarding items used to store, process, package, use and/or  
 28 distribute controlled substances, such as syringes, plastic bags, cutting agents, scales,

1 measuring equipment, chemicals or items to test the purity and/or quality of controlled  
2 substances, pill presses or encapsulating machines and associated equipment, molds, dyes,  
3 and binding agents.

4 e. Evidence relating to the acquisition, transfer, sharing, sale, or disposal  
5 of servers, email accounts, or other web services accounts used by the account holder or  
6 coconspirators to facilitate the distribution of controlled substances and the above referenced  
7 offenses.

8 f. Evidence regarding codes used in the distribution of controlled  
9 substances, including but not limited to passwords, code books, cypher or decryption keys,  
10 and similar information.

11 g. Evidence regarding payment for controlled substances, including  
12 domestic and international wire transfers (such as through Western Union), and  
13 cryptocurrency, and evidence relating to or referring to transfers or transactions of funds,  
14 including PayPal transactions.

15 h. Evidence regarding weapons, including but not limited to firearms,  
16 magazines, ammunition, and body armor.

17 i. Evidence regarding storage units, such as rental and payment records, billing  
18 information, keys and codes, pamphlets, contracts, contact information, directions, and  
19 passwords, and evidence regarding safes.

20 j. Evidence that may identify assets, including bank accounts, currency  
21 (U.S. or foreign), cryptocurrency, commodities accounts, trading accounts, tax returns,  
22 personal property, and/or real estate that may represent proceeds of the above-listed crimes,  
23 are traceable to such proceeds, or are involved in money laundering transactions.

24 k. Evidence of international or domestic travel in furtherance of the above-  
25 listed offenses.

26 l. Evidence relating to or referring to transactions through eBay or other  
27 online marketplaces;

1 m. Evidence relating to or referring to any of the following terms, aliases,  
2 or eBay usernames/user IDs:

3 i. wobra.br.kcmtwxi

4 ii. woola-bra

5 n. Evidence relating to or referring to transfers or transactions of funds,  
6 including PayPal transactions;

7 o. Evidence that serves to identify any person who uses or accesses the  
8 Target Account or who has exercised in any way any dominion or control over the Target  
9 Account.

10 p. Evidence that may reveal the current or past location of the individual or  
11 individuals using the Target Account, including all data stored in connection with location  
12 services.

13 q. Evidence indicating how and when the Target Account was accessed or  
14 used, to determine the chronological and geographic context of account access, use, and  
15 events relating to the crime under investigation and the account user.

16 r. Evidence indicating the Target Account user's state of mind as it relates  
17 to the aforementioned crimes under investigation.

18 s. Evidence relating to or referring to changes made to the account settings  
19 of any of the Target Accounts, including changes to the username/user ID, contact  
20 information, or payment information;

21 t. Evidence that may identify any alias names, online user names,  
22 "handles" and/or nicknames of those who exercise in any way any dominion or control over  
23 the Target Account.

24 u. Other log records, including IP address captures, associated with the  
25 specified account;

26 v. Subscriber records associated with the specified account, including 1)  
27 names, e-mail addresses, and screen names; 2) physical addresses; 3) records of session  
28 times and durations; 4) length of service (including start date) and types of services utilized;

1 5) telephone or instrument number or other subscriber number or identity, including any  
2 temporarily assigned network address such as internet protocol address, media access card  
3 addresses, or any other unique device identifiers recorded by Yahoo in relation to the  
4 account; 6) account log files (login IP address, account activation IP addresses, and IP  
5 address history); 7) detailed billing records/logs; 8) means and source of payment; and 9)  
6 lists of all related accounts.

7 w. Records of communications between eBay and any person purporting to  
8 be the account holder about issues relating to the account, such as technical problems, billing  
9 inquiries, or complaints from other users about the specified account. This to include records  
10 of contacts between the subscriber and the provider's support services, as well as records of  
11 any actions taken by the provider or subscriber as a result of the communications;

12 x. Information identifying accounts that are linked or associated with the  
13 Target Account.  
14  
15  
16  
17  
18  
19  
20  
21  
22  
23  
24  
25  
26  
27  
28



**ATTACHMENT A-2**

**Google Accounts to be Searched**

The electronically stored data, information and communications contained in, related to, and associated with, including all preserved data, associated with the following Google accounts (collectively, the “Target Accounts”) that are stored at premises controlled by Google LLC (“Google”), a company that is located in Mountain View, California:

- i. **bradwoolard79@gmail.com (“Target Account 2”)**
- ii. **broncosmith69@gmail.com (“Target Account 4”)**

**ATTACHMENT B-2****Items to Be Seized (Google)****I. Section I - Information to be disclosed by Google LLC for search:**

To the extent that the information described in Attachment A-2 is within the possession, custody, or control of Google LLC, regardless of whether such information is located within or outside of the United States, including any data, messages, records, files, logs, or information that has been deleted but is still available to Google LLC, or has been preserved pursuant to a request made under 18 U.S.C. § 2703(f) (please refer to preservation request numbers 1975104 and 2319572), Google LLC is required to disclose the following information to the government for each account or identifier listed in Attachment A-2, for the time period of account inception to the present:

a. The contents of all e-mails associated with the account, including stored or preserved copies of e-mails sent to and from the account, draft e-mails, the source and destination addresses associated with each e-mail, the date and time at which each e-mail was sent, and the size and length of each e-mail;

b. All subscriber records associated with the specified account, including 1) names, email addresses, and screen names; 2) physical addresses; 3) records of session times and durations; 4) length of service (including start date) and types of services utilized; 5) telephone or instrument number or other subscriber number or identity, including any temporarily assigned network address such as internet protocol address, media access card addresses, or any other unique device identifiers recorded by Google in relation to the account; 6) account log files (login IP address, account activation IP address, and IP address history); 7) detailed billing records/logs; 8) means and source of payment; and 9) lists of all related accounts;

c. any contact lists;

d. any Google Chat/Messenger information and/or records, including any contact or friend list, time, date, and IP address logs for Chat and Messenger use, and any archived web messenger communications stored on servers;

- e. any Google Calendar content;
- f. any Google Drive content (including backups of any apps stored on Google Drive;
- g. any Google Sheets content;
- h. any Google Maps content;
- i. any Google Photos content;
- j. any Google Search Console content;
- k. any Google Web & Activity content;
- l. any Google Chrome Sync content;
- m. any Google Location History content;
- n. any Google Voice content;
- o. any Android content;
- p. any Google Profile content, including all Google+ content;
- q. any account history, including any records of communications between Google and any other person about issues relating to the accounts, such as technical problems, billing inquiries, or complaints from other users about the specified account. This to include records of contacts between the subscriber and the provider's support services, as well as records of any actions taken by the provider or subscriber in connection with the service.
- r. All records or other information regarding the identification of the account, to include full name, physical address, telephone numbers and other identifiers, records of session times and durations, the date on which the account was created, the length of service, the IP address used to register the account, log-in IP addresses associated with session times and dates, account status, alternative e-mail addresses provided during registration, methods of connecting, log files, and means and source of payment (including any credit or bank account number);
- s. The types of service utilized;

1 t. All records or other information stored at any time by an individual  
 2 using the account, including address books, contact and buddy lists, calendar data, pictures,  
 3 and files;

4 u. All records pertaining to communications between the Provider and any  
 5 person regarding the account, including contacts with support services and records of actions  
 6 taken.

7  
 8 Google is hereby ordered to disclose the above information to the government within  
 9 **14 days** of service of this warrant.

10  
 11 **II. Information to be seized by the government**

12 All information described above in Section I that constitutes fruits, contraband,  
 13 evidence and instrumentalities of violations of *Distribution of, and Possession with Intent to*  
 14 *Distribute, Controlled Substances*, in violation of Title 21, United States Code, Section  
 15 841(a)(1); *Conspiracy to Distribute Controlled Substances*, in violation of Title 21, United  
 16 States Code, Sections 841(a)(1) and 846, *Money Laundering*, in violation of Title 18, United  
 17 States Code Section 1956, *Felon in Possession of a Firearm*, in violation of Title 18, United  
 18 States Code, Section 922(g), and *Distribution of controlled substances by means of the*  
 19 *internet*, in violation of Title 21, United States Code, Sections 823, 841(h)(1), 841(b)(1) and  
 20 846, those violations occurring during the period from approximately January 1, 2013 to the  
 21 present, for each of the Target Accounts listed on Attachment A-2, including the following:

22 a. Evidence that may identify any coconspirators, aiders and abettors, drug  
 23 suppliers and/or drug customers, including evidence that helps reveal their whereabouts and  
 24 including evidence of relationship(s) that existed prior to January 1, 2013.

25 b. Communications between coconspirators, sources of supply, customers,  
 26 and aiders and abettors regarding the above-referenced crimes and communications in  
 27 furtherance of the above-referenced crimes.  
 28

1 c. Evidence regarding the acquisition, importation, transportation,  
2 shipment, mailing, processing, and distribution of controlled substances.

3 d. Evidence regarding items used to store, process, package, use and/or  
4 distribute controlled substances, such as syringes, plastic bags, cutting agents, scales,  
5 measuring equipment, chemicals or items to test the purity and/or quality of controlled  
6 substances, pill presses or encapsulating machines and associated equipment, molds, dyes,  
7 and binding agents.

8 e. Evidence relating to the acquisition, transfer, sharing, sale, or disposal  
9 of servers, email accounts, or other web services accounts used by the account holder or  
10 coconspirators to facilitate the distribution of controlled substances and the above referenced  
11 offenses.

12 f. Evidence regarding codes used in the distribution of controlled  
13 substances, including but not limited to passwords, code books, cypher or decryption keys,  
14 and similar information.

15 g. Evidence regarding payment for controlled substances, including  
16 domestic and international wire transfers (such as through Western Union), and  
17 cryptocurrency, and evidence relating to or referring to transfers or transactions of funds,  
18 including PayPal transactions.

19 h. Evidence regarding weapons, including but not limited to firearms,  
20 magazines, ammunition, and body armor.

21 i. Evidence regarding storage units, such as rental and payment records, billing  
22 information, keys and codes, pamphlets, contracts, contact information, directions, and  
23 passwords, and evidence regarding safes.

24 j. Evidence that may identify assets, including bank accounts, currency  
25 (U.S. or foreign), cryptocurrency, commodities accounts, trading accounts, tax returns,  
26 personal property, and/or real estate that may represent proceeds of the above-listed crimes,  
27 are traceable to such proceeds, or are involved in money laundering transactions.



1 k. Evidence of international or domestic travel in furtherance of the above-  
2 listed offenses.

3 l. Evidence relating to or referring to transactions through eBay or other  
4 online marketplaces;

5 m. Evidence relating to or referring to any of the following terms, aliases,  
6 or eBay usernames/user IDs:

7 i. wobra.br.kcmtwxi

8 ii. woola-bra

9 n. Evidence relating to or referring to transfers or transactions of funds,  
10 including PayPal transactions;

11 o. Evidence that serves to identify any person who uses or accesses the  
12 Target Account or who has exercised in any way any dominion or control over the Target  
13 Account.

14 p. Evidence that may reveal the current or past location of the individual or  
15 individuals using the Target Account, including all data stored in connection with location  
16 services.

17 q. Evidence indicating how and when the Target Account was accessed or  
18 used, to determine the chronological and geographic context of account access, use, and  
19 events relating to the crime under investigation and the account user.

20 r. Evidence indicating the Target Account user's state of mind as it relates  
21 to the aforementioned crimes under investigation.

22 s. Evidence relating to or referring to changes made to the account settings  
23 of any of the Target Accounts, including changes to the username/user ID, contact  
24 information, or payment information;

25 t. Evidence that may identify any alias names, online user names,  
26 "handles" and/or nicknames of those who exercise in any way any dominion or control over  
27 the Target Account.  
28

1                   u.       Other log records, including IP address captures, associated with the  
2 specified account;

3                   v.       Subscriber records associated with the specified account, including 1)  
4 names, e-mail addresses, and screen names; 2) physical addresses; 3) records of session  
5 times and durations; 4) length of service (including start date) and types of services utilized;  
6 5) telephone or instrument number or other subscriber number or identity, including any  
7 temporarily assigned network address such as internet protocol address, media access card  
8 addresses, or any other unique device identifiers recorded by Yahoo in relation to the  
9 account; 6) account log files (login IP address, account activation IP addresses, and IP  
10 address history); 7) detailed billing records/logs; 8) means and source of payment; and 9)  
11 lists of all related accounts.

12                   w.       Records of communications between eBay and any person purporting to  
13 be the account holder about issues relating to the account, such as technical problems, billing  
14 inquiries, or complaints from other users about the specified account. This to include records  
15 of contacts between the subscriber and the provider's support services, as well as records of  
16 any actions taken by the provider or subscriber as a result of the communications;

17                   x.       Information identifying accounts that are linked or associated with the  
18 Target Account.  
19  
20  
21  
22  
23  
24  
25  
26  
27  
28

**ATTACHMENT A-3**

**Microsoft Accounts to be Searched**

The electronically stored data, information, and communications contained in, related to, and associated with, including all preserved data associated with the following Microsoft account (the Target Account), that are stored at premises controlled by Microsoft Corporation ("Microsoft"), a company that is located in Redmond, Washington, including any foreign data:

**greenchem201609@hotmail.com ("Target Account 3")**

**ATTACHMENT B-3****I. Section I - Information to be disclosed by Microsoft Corporation for search:**

To the extent that the information described in Attachment A-3 is within the possession, custody, or control of Microsoft, regardless of whether such information is located within or outside of the United States, including any data, messages, records, files, logs, or information that has been deleted but is still available to Microsoft, or has been preserved pursuant to a request made under Title 18, United States Code, Section 2703(f), Microsoft is required to disclose the following information to the government for the Target Account listed in Attachment A-3, from account inception to the present:

a. The contents of all e-mails associated with the account, including stored or preserved copies of e-mails sent to and from the account, draft e-mails, the source and destination addresses associated with each e-mail, the date and time at which each e-mail was sent, and the size and length of each e-mail;

b. All records or other information associated with the specified account, including 1) names, email addresses, and screen names; 2) physical addresses; 3) records of session times and durations; 4) length of service (including start date) and types of services utilized; 5) telephone or instrument number or other subscriber number or identity, including any temporarily assigned network address such as IP address, media access card addresses, or any other unique device identifiers recorded by Microsoft in relation to the account; 6) account log files (login IP address, account activation IP address, and IP address history); 7) detailed billing records/logs; 8) means and source of payment; and 9) lists of all related accounts;

c. All contact lists;

d. Any Microsoft Chat/Messenger information and/or records, including any Microsoft Chat/Messenger Friends list, time, date, and IP address logs for Chat and Messenger use, and any archived web messenger communications stored on Microsoft servers;

e. Any Microsoft Notepad information and/or records;

1 f. Any Microsoft Calendar information and/or records

2 g. Any Microsoft Groups information and/or records including member  
3 lists, e-mail addresses of members, messages, files, calendars, database content, and  
4 photographs;

5 h. Any stored documents;

6 i. All records or other information regarding the identification of the  
7 account, to include full name, physical address, telephone numbers and other identifiers,  
8 records of session times and durations, the date on which the account was created, the length  
9 of service, the IP address used to register the account, log-in IP addresses associated with  
10 session times and dates, account status, alternative e-mail addresses provided during  
11 registration, methods of connecting, log files, and means and source of payment (including  
12 any credit or bank account number);

13 j. The types of service utilized;

14 k. All records or other information stored at any time by an individual  
15 using the account, including address books, contact and buddy lists, calendar data, pictures,  
16 and files;

17 l. All account history, including any records of communications between  
18 Microsoft and any other person about issues relating to the accounts, such as technical  
19 problems, billing inquiries, or complaints from other users about the specified account. This  
20 to include records of contacts between the subscriber and the provider's support services, as  
21 well as records of any actions taken by the provider or subscriber in connection with the  
22 service.

23 Microsoft is hereby ordered to disclose the above information to the government  
24 within **14 days** of service of this warrant.

25  
26 **II. Information to be seized by the government**

27 All information described above in Section I that constitutes fruits, contraband,  
28 evidence and instrumentalities of violations of Title 21, United States Code, Section 841(a)



1 (*distribution of, and possession with intent to distribute, controlled substances*), Title 21,  
2 United States Code, Sections 841(a) and 846 (*conspiracy to distribute, and to possess with*  
3 *the intent to distribute, controlled substances*), Title 21, United States Code, Sections 823  
4 and 841(h)(1) (*distribution of controlled substances by means of the internet*), and Title 21,  
5 United States Code, Section 1956 (*money laundering*), those violations occurring between  
6 approximately January 1, 2013 and the present, for the Target Account listed on Attachment  
7 A-3, including the following:

8 a. Evidence that may identify any coconspirators, aiders and abettors, drug  
9 suppliers and/or drug customers, including evidence that helps reveal their whereabouts and  
10 including evidence of relationship(s) that existed prior to January 1, 2013.

11 b. Communications between coconspirators, sources of supply, customers,  
12 and aiders and abettors regarding the above-referenced crimes and communications in  
13 furtherance of the above-referenced crimes.

14 c. Evidence regarding the acquisition, importation, transportation,  
15 shipment, mailing, processing, and distribution of controlled substances.

16 d. Evidence regarding items used to store, process, package, use and/or  
17 distribute controlled substances, such as syringes, plastic bags, cutting agents, scales,  
18 measuring equipment, chemicals or items to test the purity and/or quality of controlled  
19 substances, pill presses or encapsulating machines and associated equipment, molds, dyes,  
20 and binding agents.

21 e. Evidence relating to the acquisition, transfer, sharing, sale, or disposal  
22 of servers, email accounts, or other web services accounts used by the account holder or  
23 coconspirators to facilitate the distribution of controlled substances and the above referenced  
24 offenses.

25 f. Evidence regarding codes used in the distribution of controlled  
26 substances, including but not limited to passwords, code books, cypher or decryption keys,  
27 and similar information.  
28

1           g. Evidence regarding payment for controlled substances, including  
2 domestic and international wire transfers (such as through Western Union), and  
3 cryptocurrency, and evidence relating to or referring to transfers or transactions of funds,  
4 including PayPal transactions.

5           h. Evidence regarding weapons, including but not limited to firearms,  
6 magazines, ammunition, and body armor.

7           i. Evidence regarding storage units, such as rental and payment records, billing  
8 information, keys and codes, pamphlets, contracts, contact information, directions, and  
9 passwords, and evidence regarding safes.

10           j. Evidence that may identify assets, including bank accounts, currency  
11 (U.S. or foreign), cryptocurrency, commodities accounts, trading accounts, tax returns,  
12 personal property, and/or real estate that may represent proceeds of the above-listed crimes,  
13 are traceable to such proceeds, or are involved in money laundering transactions.

14           k. Evidence of international or domestic travel in furtherance of the above-  
15 listed offenses.

16           l. Evidence relating to or referring to transactions through eBay or other  
17 online marketplaces;

18           m. Evidence relating to or referring to any of the following terms, aliases,  
19 or eBay usernames/user IDs:

20               i. wobra.br.kcmtwxi

21               ii. woola-bra

22           n. Evidence relating to or referring to transfers or transactions of funds,  
23 including PayPal transactions;

24           o. Evidence that serves to identify any person who uses or accesses the  
25 Target Account or who has exercised in any way any dominion or control over the Target  
26 Account.  
27  
28

1 p. Evidence that may reveal the current or past location of the individual or  
2 individuals using the Target Account, including all data stored in connection with location  
3 services.

4 q. Evidence indicating how and when the Target Account was accessed or  
5 used, to determine the chronological and geographic context of account access, use, and  
6 events relating to the crime under investigation and the account user.

7 r. Evidence indicating the Target Account user's state of mind as it relates  
8 to the aforementioned crimes under investigation.

9 s. Evidence relating to or referring to changes made to the account settings  
10 of any of the Target Accounts, including changes to the username/user ID, contact  
11 information, or payment information;

12 t. Evidence that may identify any alias names, online user names,  
13 "handles" and/or nicknames of those who exercise in any way any dominion or control over  
14 the Target Account.

15 u. Other log records, including IP address captures, associated with the  
16 specified account;

17 v. Subscriber records associated with the specified account, including 1)  
18 names, e-mail addresses, and screen names; 2) physical addresses; 3) records of session  
19 times and durations; 4) length of service (including start date) and types of services utilized;  
20 5) telephone or instrument number or other subscriber number or identity, including any  
21 temporarily assigned network address such as internet protocol address, media access card  
22 addresses, or any other unique device identifiers recorded by Yahoo in relation to the  
23 account; 6) account log files (login IP address, account activation IP addresses, and IP  
24 address history); 7) detailed billing records/logs; 8) means and source of payment; and 9)  
25 lists of all related accounts.

26 w. Records of communications between eBay and any person purporting to  
27 be the account holder about issues relating to the account, such as technical problems, billing  
28 inquiries, or complaints from other users about the specified account. This to include records

1 of contacts between the subscriber and the provider's support services, as well as records of  
2 any actions taken by the provider or subscriber as a result of the communications;

3 x. Information identifying accounts that are linked or associated with the  
4 Target Account.  
5  
6  
7  
8  
9  
10  
11  
12  
13  
14  
15  
16  
17  
18  
19  
20  
21  
22  
23  
24  
25  
26  
27  
28

**ATTACHMENT A-4**

**eBay Accounts to be Searched**

The electronically stored data, information and communications contained in, related to, and associated with, including all preserved data associated with the eBay accounts associated with the following usernames/user IDs (collectively, the “Target Accounts”) that are stored at premises controlled by eBay, Inc. (“eBay”), a company that is located in San Jose, California:

- i. **woola-bra (“Target Account 5”)**
- ii. **wobra.br.kcmtwxi (“Target Account 6”)**



**ATTACHMENT B-4****Items to Be Seized (eBay, Inc.)****I. Section I - Information to be disclosed by eBay, Inc.:**

To the extent that the information described in Attachment A-4 is within the possession, custody, or control of eBay, Inc. ("eBay"), regardless of whether such information is located within or outside of the United States, including any data, messages, records, files, logs, or information that has been deleted but is still available to eBay, or has been preserved pursuant to a request made under 18 U.S.C. § 2703(f), eBay is required to disclose the following information to the government for each account or identifier listed in Attachment A-4, from account inception to the present:

a. The contents of all e-mails or other electronic messages associated with the account, including stored or preserved copies of e-mail or message sent to and from the account, draft e-mail or message, the source and destination addresses associated with each e-mail or message, the date and time at which each e-mail or message was sent, and the size and length of each e-mail or message for the time period of account inception to the present;

b. All image files stored in the account including stored or preserved copies of files sent to and from the account, the date and time at which the file was created or received;

c. All existing printouts from original storage of all of the electronic mail or messages described above in paragraph (a);

d. All transactional information of all activity of the electronic mail addresses and/or individual accounts described above in paragraph (a), including IP connection records, log files, dates, times, methods of connecting, ports, dial-ups, and/or locations;

e. All business records and subscriber information, in any form kept, pertaining to the electronic mail addresses and/or individual accounts described above in paragraph (a), including applications, subscriber's full name, all screen names associated

1 with the subscriber and/or account, all account names associated with the subscriber,  
 2 methods of payment, telephone numbers, addresses, passwords, and detailed billing records;  
 3 and

4 f. All records indicating the services available to the subscriber of the  
 5 electronic mail address and/or individual account described above in paragraph (a).

6  
 7 eBay is hereby ordered to disclose the above information to the government within **14**  
 8 **days** of service of this warrant.

9  
 10 **II. Information to be seized by the government**

11 All information described above in Section I that constitutes fruits, contraband,  
 12 evidence and instrumentalities of violations of *Distribution of, and Possession with Intent to*  
 13 *Distribute, Controlled Substances*, in violation of Title 21, United States Code, Section  
 14 841(a)(1); *Conspiracy to Distribute Controlled Substances*, in violation of Title 21, United  
 15 States Code, Sections 841(a)(1) and 846, *Money Laundering*, in violation of Title 18, United  
 16 States Code Section 1956, *Felon in Possession of a Firearm*, in violation of Title 18, United  
 17 States Code, Section 922(g), and *Distribution of controlled substances by means of the*  
 18 *internet*, those violations occurring during the period from approximately January 1, 2013 to  
 19 the present, for each of the Target Accounts listed on Attachment A-4, including the  
 20 following:

21 **2.**

22 a. Evidence that may identify any coconspirators, aiders and abettors, drug  
 23 suppliers and/or drug customers, including evidence that helps reveal their whereabouts and  
 24 including evidence of relationship(s) that existed prior to January 1, 2013.

25 b. Communications between coconspirators, sources of supply, customers,  
 26 and aiders and abettors regarding the above-referenced crimes and communications in  
 27 furtherance of the above-referenced crimes.

1 c. Evidence regarding the acquisition, importation, transportation,  
2 shipment, mailing, processing, and distribution of controlled substances.

3 d. Evidence regarding items used to store, process, package, use and/or  
4 distribute controlled substances, such as syringes, plastic bags, cutting agents, scales,  
5 measuring equipment, chemicals or items to test the purity and/or quality of controlled  
6 substances, pill presses or encapsulating machines and associated equipment, molds, dyes,  
7 and binding agents.

8 e. Evidence relating to the acquisition, transfer, sharing, sale, or disposal  
9 of servers, email accounts, or other web services accounts used by the account holder or  
10 coconspirators to facilitate the distribution of controlled substances and the above referenced  
11 offenses.

12 f. Evidence regarding codes used in the distribution of controlled  
13 substances, including but not limited to passwords, code books, cypher or decryption keys,  
14 and similar information.

15 g. Evidence regarding payment for controlled substances, including  
16 domestic and international wire transfers (such as through Western Union), and  
17 cryptocurrency, and evidence relating to or referring to transfers or transactions of funds,  
18 including PayPal transactions.

19 h. Evidence regarding weapons, including but not limited to firearms,  
20 magazines, ammunition, and body armor.

21 i. Evidence regarding storage units, such as rental and payment records, billing  
22 information, keys and codes, pamphlets, contracts, contact information, directions, and  
23 passwords, and evidence regarding safes.

24 j. Evidence that may identify assets, including bank accounts, currency  
25 (U.S. or foreign), cryptocurrency, commodities accounts, trading accounts, tax returns,  
26 personal property, and/or real estate that may represent proceeds of the above-listed crimes,  
27 are traceable to such proceeds, or are involved in money laundering transactions.

1 k. Evidence of international or domestic travel in furtherance of the above-  
2 listed offenses.

3 l. Evidence relating to or referring to transactions through eBay or other  
4 online marketplaces;

5 m. Evidence relating to or referring to any of the following terms, aliases,  
6 or eBay usernames/user IDs:

7 i. wobra.br.kcmtwx

8 ii. woola-bra

9 n. Evidence relating to or referring to transfers or transactions of funds,  
10 including PayPal transactions;

11 o. Evidence that serves to identify any person who uses or accesses the  
12 Target Account or who has exercised in any way any dominion or control over the Target  
13 Account.

14 p. Evidence that may reveal the current or past location of the individual or  
15 individuals using the Target Account, including all data stored in connection with location  
16 services.

17 q. Evidence indicating how and when the Target Account was accessed or  
18 used, to determine the chronological and geographic context of account access, use, and  
19 events relating to the crime under investigation and the account user.

20 r. Evidence indicating the Target Account user's state of mind as it relates  
21 to the aforementioned crimes under investigation.

22 s. Evidence relating to or referring to changes made to the account settings  
23 of any of the Target Accounts, including changes to the username/user ID, contact  
24 information, or payment information;

25 t. Evidence that may identify any alias names, online user names,  
26 "handles" and/or nicknames of those who exercise in any way any dominion or control over  
27 the Target Account.

1           u.     Other log records, including IP address captures, associated with the  
2 specified account;

3           v.     Subscriber records associated with the specified account, including 1)  
4 names, e-mail addresses, and screen names; 2) physical addresses; 3) records of session  
5 times and durations; 4) length of service (including start date) and types of services utilized;  
6 5) telephone or instrument number or other subscriber number or identity, including any  
7 temporarily assigned network address such as internet protocol address, media access card  
8 addresses, or any other unique device identifiers recorded by Yahoo in relation to the  
9 account; 6) account log files (login IP address, account activation IP addresses, and IP  
10 address history); 7) detailed billing records/logs; 8) means and source of payment; and 9)  
11 lists of all related accounts.

12           w.     Records of communications between eBay and any person purporting to  
13 be the account holder about issues relating to the account, such as technical problems, billing  
14 inquiries, or complaints from other users about the specified account. This to include records  
15 of contacts between the subscriber and the provider's support services, as well as records of  
16 any actions taken by the provider or subscriber as a result of the communications;

17           x.     Information identifying accounts that are linked or associated with the  
18 Target Account.  
19  
20  
21  
22  
23  
24  
25  
26  
27  
28

**CERTIFICATE OF AUTHENTICITY OF BUSINESS RECORDS**  
**PURSUANT TO FEDERAL RULES OF EVIDENCE 902(11) AND 902(13)**

I, \_\_\_\_\_, attest, under penalties of perjury by the laws of the United States of America pursuant to 28 U.S.C. § 1746, that the information contained in this certification is true and correct. I am employed by \_\_\_\_\_, and my title is \_\_\_\_\_. I am qualified to authenticate the records attached hereto because I am familiar with how the records were created, managed, stored, and retrieved. I state that the records attached hereto are true duplicates of the original records in the custody of \_\_\_\_\_.

The attached records consist of \_\_\_\_\_ [GENERALLY DESCRIBE RECORDS (pages/CDs/megabytes)]. I further state that:

a. All records attached to this certificate were made at or near the time of the occurrence of the matter set forth by, or from information transmitted by, a person with knowledge of those matters, they were kept in the ordinary course of the regularly conducted business activity of \_\_\_\_\_, and they were made by \_\_\_\_\_ as a regular practice; and .

b. Such records were generated by \_\_\_\_\_'s electronic process or system that produces an accurate result, to wit:

1. The records were copied from electronic device(s), storage medium(s), or file(s) in the custody of \_\_\_\_\_ in a manner to ensure that they are true duplicates of the original records; and

2. The process or system is regularly verified by \_\_\_\_\_, and at all times pertinent to the records certified here the process and system functioned properly and normally.

//

//



1 I further state that this certification is intended to satisfy Rules 902(11) and  
2 902(13) of the Federal Rules of Evidence.

3  
4  
5 \_\_\_\_\_  
6 Date

Signature  
7  
8  
9  
10  
11  
12  
13  
14  
15  
16  
17  
18  
19  
20  
21  
22  
23  
24  
25  
26  
27  
28